PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-152698

(43)Date of publication of application : 23.05.2003

(51)Int.Cl. H04L 9/08
H04H 1/00
H04L 9/16
H04N 7/08
H04N 7/081
H04N 7/167

(21)Application number : 2001-349539

(22)Date of filing : 15.11.2001

(71)Applicant : NIPPON HOSO KYOKAI <NHK>

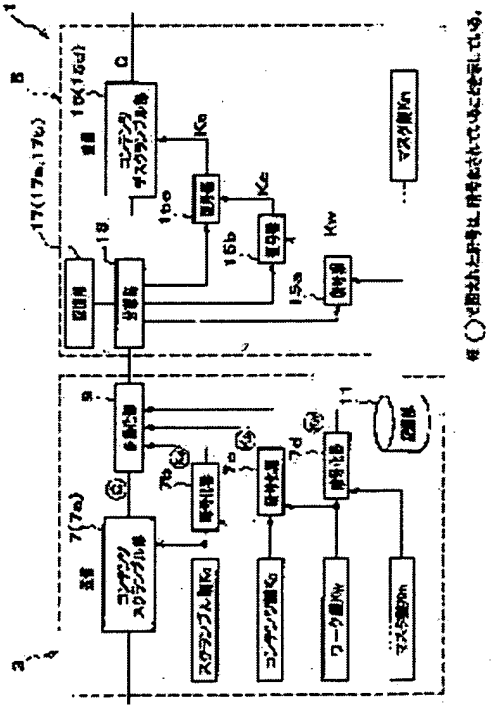
(72)Inventor : NISHIMOTO TOMONARI
KURIOKA TATSUYA
UEHARA TOSHIHIRO
NANBA SEIICHI
OKUDA HARUO

(54) CONTENTS UTILIZATION CONTROL TRANSMITTING METHOD, CONTENTS UTILIZATION CONTROL RECEIVING METHOD, CONTENTS UTILIZATION CONTROL TRANSMITTING DEVICE, CONTENTS UTILIZATION CONTROL RECEIVING DEVICE, CONTENTS UTILIZATION CONTROL TRANSMITTING PROGRAM AND CONTENTS UTILIZATION CONTROL RECEIVING PROGRAM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a contents utilization control transmitting method, receiving method, contents utilization control transmitting device, receiving device, contents utilization control transmitting program and receiving program in which the illegal utilization of contents can be prevented even when a receiver on a receiving side is illegally altered or illegally produced.

SOLUTION: A system is composed of a contents utilization control transmitting device 3 for transmitting encrypted contents in which contents are encrypted, reproduction order control information for controlling the reproduction order of the relevant encrypted contents and viewing control information for controlling viewing of the relevant encrypted contents and a contents utilization control receiving device 5 for receiving such information, the transmitting device 3 is provided with a contents scramble part 7, a multiplexing part 9 and a storage part 11, and the receiving device 5 is provided with a demultiplexing part 13, a contents descramble part 15 and a storage part 17.



LEGAL STATUS

[Date of request for examination] 09.04.2004

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application

converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2003－152698
（P2003－152698A）
(43)公開日　平成15年５月23日(2003.5.23)

(51)Int.Cl.⁷		識別記号	Ｆ Ｉ			ﾃｰﾏｺｰﾄﾞ(参考)
Ｈ０４Ｌ	9/08		Ｈ０４Ｈ	1/00	Ｆ	５Ｃ０６３
Ｈ０４Ｈ	1/00		Ｈ０４Ｌ	9/00	６０１Ｂ	５Ｃ０６４
Ｈ０４Ｌ	9/16		Ｈ０４Ｎ	7/08	Ｚ	５Ｊ１０４
Ｈ０４Ｎ	7/08			7/167	Ｚ	
	7/081		Ｈ０４Ｌ	9/00	６４３	

審査請求　未請求　請求項の数15　ＯＬ　（全 26 頁）　最終頁に続く

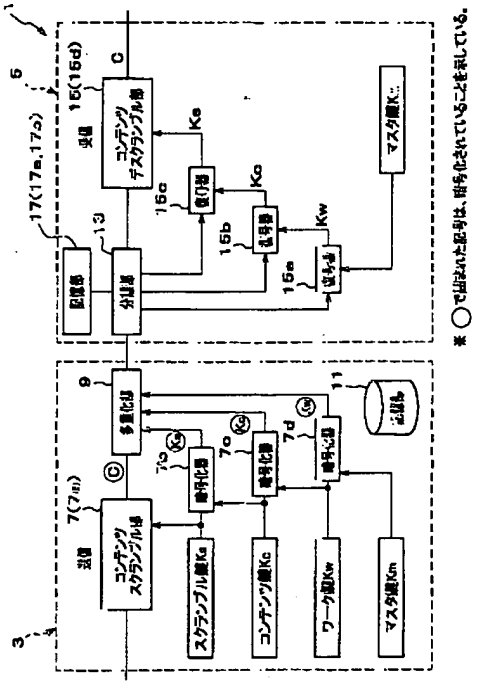
(21)出願番号　特願2001－349539(P2001－349539)
(22)出願日　平成13年11月15日(2001.11.15)

(71)出願人　000004352
日本放送協会
東京都渋谷区神南２丁目２番１号
(72)発明者　西本　友成
東京都世田谷区砧一丁目10番11号　日本放送協会　放送技術研究所内
(72)発明者　栗岡　辰弥
東京都世田谷区砧一丁目10番11号　日本放送協会　放送技術研究所内
(74)代理人　100064414
弁理士　磯野　道造

最終頁に続く

(54)【発明の名称】　コンテンツ利用制御送信方法、コンテンツ利用制御受信方法およびコンテンツ利用制御送信装置、コンテンツ利用制御受信装置ならびにコンテンツ利用制御送信プログラム、コンテンツ利用

(57)【要約】
【課題】　受信側の受信機が不正に改造されたり不正に製造されたものであっても、コンテンツの不正利用を防止することができるコンテンツ利用制御送信方法、受信方法、コンテンツ利用制御送信装置、受信装置、コンテンツ利用制御送信プログラム、受信プログラムを提供する。
【解決手段】　コンテンツを暗号化した暗号化コンテンツと、当該暗号化コンテンツの再生順序を制御する再生順序制御情報および当該暗号化コンテンツの視聴を制御する視聴制御情報と、を送信するコンテンツ利用制御送信装置３、これらの情報を受信するコンテンツ利用制御受信装置５によって構成し、送信装置３は、コンテンツスクランブル部７と多重化部９と記憶部１１とを備え、受信装置５は、分離部１３とコンテンツデスクランブル部１５と記憶部１７とを備えた。



【特許請求の範囲】

【請求項１】　デジタル放送におけるコンテンツを暗号化した暗号化コンテンツと、受信側で当該暗号化コンテンツの利用を制御する利用制御情報とを送信するコンテンツ利用制御送信方法であって、

経過時間に伴って変更されるスクランブル鍵により、前記コンテンツを暗号化して暗号化コンテンツとするコンテンツ暗号化ステップと、

共通鍵暗号化方式に供される共通鍵により、少なくとも前記利用制御情報および前記スクランブル鍵を含む関連情報を暗号化し暗号化関連情報とする関連情報暗号化ステップと、

前記暗号化コンテンツ、前記暗号化関連情報を多重化し多重暗号コンテンツとする多重化ステップと、

この多重化ステップで多重化された多重化暗号コンテンツを送信する多重化暗号コンテンツ送信ステップと、を含むことを特徴とするコンテンツ利用制御送信方法。

【請求項２】　前記利用制御情報は、当該暗号化コンテンツの再生順序を制御する再生順序制御情報と、当該暗号化コンテンツの視聴を制御する視聴制御情報との少なくとも一方の情報を含んでいることを特徴とする請求項１に記載のコンテンツ利用制御送信方法。

【請求項３】　デジタル放送におけるコンテンツを暗号化した暗号化コンテンツと、受信側で当該暗号化コンテンツの再生順序を制御する再生順序制御情報および当該暗号化コンテンツの視聴を制御する視聴制御情報と、を送信するコンテンツ利用制御送信方法であって、

経過時間に伴って変更されるスクランブル鍵により、前記コンテンツを暗号化して暗号化コンテンツとするコンテンツ暗号化ステップと、

前記コンテンツ毎に設けられたコンテンツ鍵により、少なくとも前記再生順序制御情報および前記スクランブル鍵を含む関連情報を暗号化し暗号化関連情報とする関連情報暗号化ステップと、

前記コンテンツの継続時間を越えて保持されるワーク鍵により、少なくとも前記視聴制御情報および前記コンテンツ鍵を含む当該コンテンツ鍵に関するコンテンツ鍵関連情報を暗号化し暗号化コンテンツ鍵関連情報とするコンテンツ鍵関連情報暗号化ステップと、

受信側に共通に備えられるマスター鍵により、少なくとも前記ワーク鍵を含むワーク鍵に関するワーク鍵関連情報を暗号化し暗号化ワーク鍵関連情報とするワーク鍵関連情報暗号化ステップと、

前記暗号化コンテンツ、前記暗号化関連情報、前記暗号化コンテンツ鍵関連情報、前記暗号化ワーク鍵関連情報を多重化した多重化暗号コンテンツとする多重化ステップと、

この多重化ステップで多重化された多重化暗号コンテンツを送信する多重化暗号コンテンツ送信ステップと、を含むことを特徴とするコンテンツ利用情報送信方法。

【請求項４】　経過時間に伴って変更されるスクランブル鍵によりデジタル放送におけるコンテンツを暗号化した暗号化コンテンツと、共通鍵暗号化方式に供される共通鍵により、少なくとも当該暗号化コンテンツの利用を制御する利用制御情報および前記スクランブル鍵を含む関連情報を暗号化した暗号化関連情報とを送信側で多重化した多重化暗号コンテンツを受信するコンテンツ利用制御受信方法であって、

前記多重化暗号コンテンツを受信する多重化暗号コンテンツ受信ステップと、

この多重化暗号コンテンツ受信ステップで受信した多重化暗号コンテンツを、前記暗号化コンテンツ、前記暗号化関連情報に分離する多重化暗号コンテンツ分離ステップと、

この多重化暗号コンテンツ分離ステップで分離された暗号化関連情報に含まれている暗号化スクランブル鍵および暗号化利用制御情報を、前記共通鍵により復号する暗号化利用制御情報復号ステップと、

この暗号化利用制御情報復号ステップで復号された利用制御情報に基づいて、前記スクランブル鍵により前記暗号化コンテンツを復号する暗号化コンテンツ復号ステップと、を含むことを特徴とするコンテンツ利用制御受信方法。

【請求項５】　経過時間に伴って変更されるスクランブル鍵によりデジタル放送におけるコンテンツを暗号化した暗号化コンテンツと、前記コンテンツ毎に設けられたコンテンツ鍵により少なくとも当該暗号化コンテンツの再生順序を制御する再生順序制御情報および前記スクランブル鍵を含む関連情報を暗号化した暗号化関連情報と、前記コンテンツの継続時間を越えて保持されるワーク鍵により少なくとも当該暗号化コンテンツの視聴を制御する視聴制御情報および前記コンテンツ鍵を含む当該コンテンツ鍵に関するコンテンツ鍵関連情報を暗号化した暗号化コンテンツ鍵関連情報と、送信側に共通に備えられるマスター鍵により少なくとも前記ワーク鍵を含むワーク鍵に関するワーク鍵関連情報を暗号化した暗号化ワーク鍵関連情報とを送信側で多重化した多重化暗号コンテンツを受信するコンテンツ利用制御受信方法であって、

前記多重化暗号コンテンツを受信する多重化暗号コンテンツ受信ステップと、

この多重化暗号コンテンツ受信ステップで受信した多重化暗号コンテンツを、前記暗号化コンテンツ、前記暗号化関連情報、前記暗号化コンテンツ鍵関連情報、前記暗号化ワーク鍵関連情報に分離する多重化暗号コンテンツ分離ステップと、

この多重化暗号コンテンツ分離ステップで分離された暗号化ワーク鍵関連情報を前記マスター鍵で復号しワーク鍵を得る暗号化ワーク鍵関連情報復号ステップと、

この暗号化ワーク鍵関連情報復号ステップで得られたワ

ーク鍵で暗号化コンテンツ鍵関連情報に含まれている暗号化コンテンツ鍵および暗号化視聴制御情報を復号しコンテンツ鍵および視聴制御情報を得る暗号化コンテンツ鍵関連情報復号ステップと、
この暗号化コンテンツ鍵関連情報復号ステップで復号された視聴制御情報に基づいて、前記暗号化関連情報に含まれている暗号化スクランブル鍵および暗号化再生順序制御情報を復号しスクランブル鍵および再生順序制御情報を得る暗号化関連情報復号ステップと、
この暗号化関連情報復号ステップで復号された再生順序制御情報に基づいて、復号されたスクランブル鍵により前記暗号化コンテンツを復号する暗号化コンテンツ復号ステップと、を含むことを特徴とするコンテンツ利用制御受信方法。

【請求項６】　デジタル放送におけるコンテンツを暗号化した暗号化コンテンツと、受信側で当該暗号化コンテンツの利用を制御する利用制御情報とを送信するコンテンツ利用制御送信装置であって、
経過時間に伴って変更されるスクランブル鍵を生成するスクランブル鍵生成手段と、
共通鍵暗号化方式に供される共通鍵を記憶する記憶手段と、
前記スクランブル鍵により、前記コンテンツを暗号化して暗号化コンテンツとするコンテンツ暗号化手段と、
前記共通鍵により、少なくとも前記利用制御情報および前記スクランブル鍵を含む関連情報を暗号化し暗号化関連情報とする関連情報暗号化手段と、
前記暗号化コンテンツ、前記暗号化関連情報を多重化し多重暗号コンテンツとする多重化手段と、
この多重化手段で多重化された多重化暗号コンテンツを送信する多重化暗号コンテンツ送信手段と、を備えることを特徴とするコンテンツ利用制御送信装置。

【請求項７】　前記利用制御情報は、当該暗号化コンテンツの再生順序を制御する再生順序制御情報と、当該暗号化コンテンツの視聴を制御する視聴制御情報との少なくとも一方の情報を含んでいることを特徴とする請求項６に記載のコンテンツ利用制御送信装置。

【請求項８】　デジタル放送におけるコンテンツを暗号化した暗号化コンテンツと、受信側で当該暗号化コンテンツの再生順序を制御する再生順序制御情報および当該暗号化コンテンツの視聴を制御する視聴制御情報と、を送信するコンテンツ利用制御送信装置であって、
経過時間に伴って変更されるスクランブル鍵を生成するスクランブル鍵生成手段と、
前記コンテンツ毎に設けられたコンテンツ鍵、前記コンテンツの継続時間を越えて保持されるワーク鍵、受信側に共通に備えられるマスター鍵を記憶する記憶手段と、
前記スクランブル鍵により、前記コンテンツを暗号化して暗号化コンテンツとするコンテンツ暗号化手段と、
前記コンテンツ鍵により、少なくとも前記再生順序制御情報および前記スクランブル鍵を含む関連情報を暗号化し暗号化関連情報とする関連情報暗号化手段と、
前記ワーク鍵により、少なくとも前記視聴制御情報および前記コンテンツ鍵を含む当該コンテンツ鍵に関するコンテンツ鍵関連情報を暗号化し暗号化コンテンツ鍵関連情報とするコンテンツ鍵関連情報暗号化手段と、
前記マスター鍵により、少なくとも前記ワーク鍵を含むワーク鍵に関するワーク鍵関連情報を暗号化し暗号化ワーク鍵関連情報とするワーク鍵関連情報暗号化手段と、
前記暗号化コンテンツ、前記暗号化関連情報、前記暗号化コンテンツ鍵関連情報、前記暗号化ワーク鍵関連情報を多重化した多重化暗号コンテンツとする多重化手段と、
この多重化手段で多重化された多重化暗号コンテンツを送信する多重化暗号コンテンツ送信手段と、を備えることを特徴とするコンテンツ利用制御送信装置。

【請求項９】　経過時間に伴って変更されるスクランブル鍵によりデジタル放送におけるコンテンツを暗号化した暗号化コンテンツと、共通鍵暗号化方式に供される共通鍵により、少なくとも当該暗号化コンテンツの利用を制御する利用制御情報および前記スクランブル鍵を含む関連情報を暗号化した暗号化関連情報とを送信側で多重化した多重化暗号コンテンツを受信するコンテンツ利用制御受信装置であって、
前記多重化暗号コンテンツを受信する多重化暗号コンテンツ受信手段と、
この多重化暗号コンテンツ受信手段で受信した多重化暗号コンテンツを、前記暗号化コンテンツ、前記暗号化関連情報に分離する多重化暗号コンテンツ分離手段と、
この多重化暗号コンテンツ分離手段で分離された暗号化関連情報に含まれている暗号化スクランブル鍵および暗号化利用制御情報を、前記共通鍵により復号する暗号化利用制御情報復号手段と、
この暗号化利用制御情報復号手段で復号された利用制御情報に基づいて、復号されたスクランブル鍵により前記暗号化コンテンツを復号する暗号化コンテンツ復号手段と、を備えることを特徴とするコンテンツ利用制御受信装置。

【請求項１０】　経過時間に伴って変更されるスクランブル鍵によりデジタル放送におけるコンテンツを暗号化した暗号化コンテンツと、前記コンテンツ毎に設けられたコンテンツ鍵により少なくとも当該暗号化コンテンツの再生順序を制御する再生順序制御情報および前記スクランブル鍵を含む関連情報を暗号化した暗号化関連情報と、前記コンテンツの継続時間を越えて保持されるワーク鍵により少なくとも当該暗号化コンテンツの視聴を制御する視聴制御情報および前記コンテンツ鍵を含む当該コンテンツ鍵に関するコンテンツ鍵関連情報を暗号化した暗号化コンテンツ鍵関連情報と、送信側に共通に備えられるマスター鍵により少なくとも前記ワーク鍵を含む

ワーク鍵に関するワーク鍵関連情報を暗号化した暗号化ワーク鍵関連情報とを送信側で多重化した多重化暗号コンテンツを受信するコンテンツ利用制御受信装置であって、
前記多重化暗号コンテンツを受信する多重化暗号コンテンツ受信手段と、
この多重化暗号コンテンツ受信手段で受信した多重化暗号コンテンツを、前記暗号化コンテンツ、前記暗号化関連情報、前記暗号化コンテンツ鍵関連情報、前記暗号化ワーク鍵関連情報に分離する多重化暗号コンテンツ分離手段と、
この多重化暗号コンテンツ分離手段で分離された暗号化ワーク鍵関連情報を前記マスター鍵で復号しワーク鍵を得る暗号化ワーク鍵関連情報復号手段と、
この暗号化ワーク鍵関連情報復号手段で得られたワーク鍵で暗号化コンテンツ鍵関連情報に含まれている暗号化コンテンツ鍵および暗号化視聴制御情報を復号しコンテンツ鍵および視聴制御情報を得る暗号化コンテンツ鍵関連情報復号手段と、
この暗号化コンテンツ鍵関連情報復号手段で復号された視聴制御情報に基づいて、前記暗号化関連情報に含まれている暗号化スクランブル鍵および暗号化再生順序制御情報を復号しスクランブル鍵および再生順序制御情報を得る暗号化関連情報復号手段と、
この暗号化関連情報復号手段で復号された再生順序制御情報に基づいて、復号されたスクランブル鍵により前記暗号化コンテンツを復号する暗号化コンテンツ復号手段と、を備えることを特徴とするコンテンツ利用制御受信装置。

【請求項１１】　デジタル放送におけるコンテンツを暗号化した暗号化コンテンツと、受信側で当該暗号化コンテンツの利用を制御する利用制御情報とを送信するコンテンツ利用制御送信装置を、
経過時間に伴って変更されるスクランブル鍵を生成するスクランブル鍵生成手段、
共通鍵暗号化方式に供される共通鍵を記憶する記憶手段、
前記スクランブル鍵により、前記コンテンツを暗号化して暗号化コンテンツとするコンテンツ暗号化手段、
前記共通鍵により、少なくとも前記利用制御情報および前記スクランブル鍵を含む関連情報を暗号化し暗号化関連情報とする関連情報暗号化手段、
前記暗号化コンテンツ、前記暗号化関連情報を多重化し多重暗号コンテンツとする多重化手段、
この多重化手段で多重化された多重化暗号コンテンツを送信する多重化暗号コンテンツ送信手段、として機能させることを特徴とするコンテンツ利用制御送信プログラム。

【請求項１２】　請求項１１に記載のコンテンツ利用制御送信プログラムにおいて、前記利用制御情報は、当該暗号化コンテンツの再生順序を制御する再生順序制御情報と、当該暗号化コンテンツの視聴を制御する視聴制御情報との少なくとも一方の情報を含んでいることを特徴とするコンテンツ利用制御送信プログラム。

【請求項１３】　デジタル放送におけるコンテンツを暗号化した暗号化コンテンツと、受信側で当該暗号化コンテンツの再生順序を制御する再生順序制御情報および当該暗号化コンテンツの視聴を制御する視聴制御情報と、を送信するコンテンツ利用制御送信装置を、
経過時間に伴って変更されるスクランブル鍵を生成するスクランブル鍵生成手段、
前記コンテンツ毎に設けられたコンテンツ鍵、前記コンテンツの継続時間を越えて保持されるワーク鍵、受信側に共通に備えられるマスター鍵を記憶する記憶手段、
前記スクランブル鍵により、前記コンテンツを暗号化して暗号化コンテンツとするコンテンツ暗号化手段、
前記コンテンツ鍵により、少なくとも前記再生順序制御情報および前記スクランブル鍵を含む関連情報を暗号化し暗号化関連情報とする関連情報暗号化手段、
前記ワーク鍵により、少なくとも前記視聴制御情報および前記コンテンツ鍵を含む当該コンテンツ鍵に関するコンテンツ鍵関連情報を暗号化し暗号化コンテンツ鍵関連情報とするコンテンツ鍵関連情報暗号化手段、
前記マスター鍵により、少なくとも前記ワーク鍵を含むワーク鍵に関するワーク鍵関連情報を暗号化し暗号化ワーク鍵関連情報とするワーク鍵関連情報暗号化手段、
前記暗号化コンテンツ、前記暗号化関連情報、前記暗号化コンテンツ鍵関連情報、前記暗号化ワーク鍵関連情報を多重化した多重化暗号コンテンツとする多重化手段、
この多重化手段で多重化された多重化暗号コンテンツを送信する多重化暗号コンテンツ送信手段、として機能させることを特徴とするコンテンツ利用制御送信プログラム。

【請求項１４】　経過時間に伴って変更されるスクランブル鍵によりデジタル放送におけるコンテンツを暗号化した暗号化コンテンツと、共通鍵暗号化方式に供される共通鍵により、少なくとも当該暗号化コンテンツの利用を制御する利用制御情報および前記スクランブル鍵を含む関連情報を暗号化した暗号化関連情報とを送信側で多重化した多重化暗号コンテンツを受信するコンテンツ利用制御受信装置を、
前記多重化暗号コンテンツを受信する多重化暗号コンテンツ受信手段、
この多重化暗号コンテンツ受信手段で受信した多重化暗号コンテンツを、前記暗号化コンテンツ、前記暗号化関連情報に分離する多重化暗号コンテンツ分離手段、
この多重化暗号コンテンツ分離手段で分離された暗号化関連情報に含まれている暗号化スクランブル鍵および暗号化利用制御情報を、前記共通鍵により復号する暗号化利用制御情報復号手段、

この暗号化利用制御情報復号手段で復号された利用制御情報に基づいて、復号されたスクランブル鍵により前記暗号化コンテンツを復号する暗号化コンテンツ復号手段、として機能させることを特徴とするコンテンツ利用制御受信プログラム。

【請求項１５】　経過時間に伴って変更されるスクランブル鍵によりデジタル放送におけるコンテンツを暗号化した暗号化コンテンツと、前記コンテンツ毎に設けられたコンテンツ鍵により少なくとも当該暗号化コンテンツの再生順序を制御する再生順序制御情報および前記スクランブル鍵を含む関連情報を暗号化した暗号化関連情報と、前記コンテンツの継続時間を越えて保持されるワーク鍵により少なくとも当該暗号化コンテンツの視聴を制御する視聴制御情報および前記コンテンツ鍵を含む当該コンテンツ鍵に関するコンテンツ鍵関連情報を暗号化した暗号化コンテンツ鍵関連情報と、送信側に共通に備えられるマスター鍵により少なくとも前記ワーク鍵を含むワーク鍵に関するワーク鍵関連情報を暗号化した暗号化ワーク鍵関連情報とを送信側で多重化した多重化暗号コンテンツを受信するコンテンツ利用制御受信装置を、

前記多重化暗号コンテンツを受信する多重化暗号コンテンツ受信手段、

この多重化暗号コンテンツ受信手段で受信した多重化暗号コンテンツを、前記暗号化コンテンツ、前記暗号化関連情報、前記暗号化コンテンツ鍵関連情報、前記暗号化ワーク鍵関連情報に分離する多重化暗号コンテンツ分離手段、

この多重化暗号コンテンツ分離手段で分離された暗号化ワーク鍵関連情報を前記マスター鍵で復号しワーク鍵を得る暗号化ワーク鍵関連情報復号手段、

この暗号化ワーク鍵関連情報復号手段で得られたワーク鍵で暗号化コンテンツ鍵関連情報に含まれている暗号化コンテンツ鍵および暗号化視聴制御情報を復号しコンテンツ鍵および視聴制御情報を得る暗号化コンテンツ鍵関連情報復号手段、

この暗号化コンテンツ鍵関連情報復号手段で復号された視聴制御情報に基づいて、前記暗号化関連情報に含まれている暗号化スクランブル鍵および暗号化再生順序制御情報を復号しスクランブル鍵および再生順序制御情報を得る暗号化関連情報復号手段、

この暗号化関連情報復号手段で復号された再生順序制御情報に基づいて、復号されたスクランブル鍵により前記暗号化コンテンツを復号する暗号化コンテンツ復号手段、として機能させることを特徴とするコンテンツ利用制御受信プログラム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、デジタル放送におけるコンテンツの利用を制御するコンテンツ利用制御送信方法、コンテンツ利用制御受信方法およびコンテンツ利用制御送信装置、コンテンツ利用制御受信装置ならびにコンテンツ利用制御送信プログラム、コンテンツ利用制御受信プログラムに関する。

【０００２】

【従来の技術】近年、デジタル放送におけるコンテンツ（デジタルコンテンツ）を、受信側で大容量のハードディスク等のランダムアクセス可能な蓄積装置に蓄積し、利用（再生、編集等）するサービス（コンテンツの視聴）が想定されている。このサービスは、ランダムアクセス可能な蓄積装置にコンテンツを蓄積させ、コンテンツのあるシーンのみ（視聴者が所望するシーン）をノンリニアに再生させることにより、実現可能になるものである。

【０００３】また、デジタル放送におけるコンテンツには、コンテンツ中に各シーンに対応するメタデータ（コンテンツに関する情報：特にコンテンツ（番組）内の各シーンの見出しに相当する番組内インデックス）が付されており、このメタデータが付されたコンテンツが送信側から送信され、受信側で当該メタデータをコンテンツ検索（コンテンツの特定シーンの検索）に利用されることが想定されている。

【０００４】

【発明が解決しようとする課題】ところが、ランダムアクセス可能な蓄積装置にコンテンツが蓄積されることによって実現されるサービスは、受信者側の視聴者に対して便利なサービスである一方、送信者側の放送局（コンテンツ制作者）にとっては、放送局（コンテンツ制作者）の意図しないコンテンツの利用が行われる（コンテンツの不正利用）可能性がある。例えば、コンテンツ中に含まれているＣＭ等のコンテンツの一部が意図的にスキップされ（削除され）視聴される恐れがある。また、送信側でコンテンツに付されたメタデータを、受信側で悪意を持った視聴者が不正に改ざんしたり、別のメタデータを付してコンテンツを利用する（コンテンツの不正利用）恐れがある。

【０００５】従来、このようなコンテンツの不正利用を防止するための方策（防止策）として、コンテンツ中のシーンやＣＭをスキップをさせない為の制御信号を、コンテンツと併せて（多重化して）送信側から送信し、受信側の受信機で当該制御信号に従って、当該受信機を動作させることで、コンテンツを視聴することが想定されている。

【０００６】しかしながら、従来のコンテンツの不正利用の防止策では、送信側で多重化された制御信号に従って、受信側の受信機が制御されることが前提となっているが、受信側の受信機が不正に改造されていたり、不正に製造されたものであった場合、送信側で多重化された制御信号は有効に機能しないことが想定される。

【０００７】そこで、本発明の目的は前記した従来の技術が有する課題を解消し、受信側の受信機が不正に改造

されたり不正に製造されたものであっても、コンテンツの不正利用を防止することができるコンテンツ利用制御送信方法、コンテンツ利用制御受信方法およびコンテンツ利用制御送信装置、コンテンツ利用制御受信装置ならびにコンテンツ利用制御送信プログラム、コンテンツ利用制御受信プログラムを提供することにある。

【０００８】

【課題を解決するための手段】前記した目的を達成するため、以下に示す構成とした。請求項１記載のコンテンツ利用制御送信方法は、デジタル放送におけるコンテンツを暗号化した暗号化コンテンツと、受信側で当該暗号化コンテンツの利用を制御する利用制御情報とを送信するコンテンツ利用制御送信方法であって、経過時間に伴って変更されるスクランブル鍵により、前記コンテンツを暗号化して暗号化コンテンツとするコンテンツ暗号化ステップと、共通鍵暗号化方式に供される共通鍵により、少なくとも前記利用制御情報および前記スクランブル鍵を含む関連情報を暗号化し暗号化関連情報とする関連情報暗号化ステップと、前記暗号化コンテンツ、前記暗号化関連情報を多重化し多重暗号コンテンツとする多重化ステップと、この多重化ステップで多重化された多重化暗号コンテンツを送信する多重化暗号コンテンツ送信ステップと、を含むことを特徴とする。

【０００９】この方法では、まず、コンテンツ暗号化ステップにおいて、経過時間に伴って変更されるスクランブル鍵によってコンテンツが暗号化され暗号化コンテンツとされる。一方、スクランブル鍵を含む関連情報と利用制御情報とが、共通鍵暗号化方式に供される共通鍵によって暗号化され暗号化関連情報とされる。そして、これらが多重化ステップにおいて多重化され多重化暗号コンテンツとされ、多重化暗号コンテンツ送信ステップで送信される。

【００１０】また、請求項２記載のコンテンツ利用制御送信方法は、請求項１に記載のコンテンツ利用制御送信方法において、前記利用制御情報は、当該暗号化コンテンツの再生順序を制御する再生順序制御情報と、当該暗号化コンテンツの視聴を制御する視聴制御情報との少なくとも一方の情報を含んでいることを特徴とする。

【００１１】この方法では、利用制御情報が再生順序制御情報と視聴制御情報との少なくとも一方の情報を含んでいるので、受信側でコンテンツを利用するときに、この情報に従って、送信側の意図するようにコンテンツの利用制御がなされる。

【００１２】また、請求項３記載のコンテンツ利用制御送信方法は、デジタル放送におけるコンテンツを暗号化した暗号化コンテンツと、受信側で当該暗号化コンテンツの再生順序を制御する再生順序制御情報および当該暗号化コンテンツの視聴を制御する視聴制御情報と、を送信するコンテンツ利用制御送信方法であって、経過時間に伴って変更されるスクランブル鍵により、前記コンテンツを暗号化して暗号化コンテンツとするコンテンツ暗号化ステップと、前記コンテンツ毎に設けられたコンテンツ鍵により、少なくとも前記再生順序制御情報および前記スクランブル鍵を含む関連情報を暗号化し暗号化関連情報とする関連情報暗号化ステップと、前記コンテンツの継続時間を越えて保持されるワーク鍵により、少なくとも前記視聴制御情報および前記コンテンツ鍵を含む当該ゴンテンツ鍵に関するコンテンツ鍵関連情報を暗号化し暗号化コンテンツ鍵関連情報とするコンテンツ鍵関連情報暗号化ステップと、受信側に共通に備えられるマスター鍵により、少なくとも前記ワーク鍵を含むワーク鍵に関するワーク鍵関連情報を暗号化し暗号化ワーク鍵関連情報とするワーク鍵関連情報暗号化ステップと、前記暗号化コンテンツ、前記暗号化関連情報、前記暗号化コンテンツ鍵関連情報、前記暗号化ワーク鍵関連情報を多重化した多重化暗号コンテンツとする多重化ステップと、この多重化ステップで多重化された多重化暗号コンテンツを送信する多重化暗号コンテンツ送信ステップと、を含むことを特徴とする。

【００１３】この方法では、まず、コンテンツ暗号化ステップにおいて、経過時間に伴って変更されるスクランブル鍵によって、コンテンツが暗号化され暗号化コンテンツとされる。次に、関連情報暗号化ステップにおいて、コンテンツ毎に設けられたコンテンツ鍵によって、少なくとも再生順序制御情報およびスクランブル鍵を含む関連情報が暗号化され暗号化関連情報とされる。また、コンテンツ鍵関連情報情報暗号化ステップにおいて、コンテンツの継続時間を越えて保持されるワーク鍵によって、少なくとも視聴制御情報およびコンテンツ鍵を含む当該コンテンツ鍵に関するコンテンツ鍵関連情報が暗号化され暗号化コンテンツ鍵関連情報とされる。さらに、ワーク鍵関連情報暗号化ステップにおいて、受信側に共通に備えられるマスター鍵によって、少なくともワーク鍵を含むワーク鍵に関するワーク鍵関連情報が暗号化され暗号化ワーク鍵関連情報とされる。そして、多重化ステップにおいて、暗号化コンテンツ、暗号化関連情報、暗号化コンテンツ鍵関連情報、暗号化ワーク鍵関連情報が多重化され多重化暗号コンテンツとされ、多重化暗号コンテンツ送信ステップで、この多重化暗号コンテンツが送信される。

【００１４】さらに、請求項４記載のコンテンツ利用制御受信方法は、経過時間に伴って変更されるスクランブル鍵によりデジタル放送におけるコンテンツを暗号化した暗号化コンテンツと、共通鍵暗号化方式に供される共通鍵により、少なくとも当該暗号化コンテンツの利用を制御する利用制御情報および前記スクランブル鍵を含む関連情報を暗号化した暗号化関連情報とを送信側で多重化した多重化暗号コンテンツを受信するコンテンツ利用制御受信方法であって、前記多重化暗号コンテンツを受信する多重化暗号コンテンツ受信ステップと、この多重

化暗号コンテンツ受信ステップで受信した多重化暗号コンテンツを、前記暗号化コンテンツ、前記暗号化関連情報に分離する多重化暗号コンテンツ分離ステップと、この多重化暗号コンテンツ分離ステップで分離された暗号化関連情報に含まれている暗号化スクランブル鍵および暗号化利用制御情報を、前記共通鍵により復号する暗号化利用制御情報復号ステップと、この暗号化利用制御情報復号ステップで復号された利用制御情報に基づいて、前記スクランブル鍵により前記暗号化コンテンツを復号する暗号化コンテンツ復号ステップと、を含むことを特徴とする。

【００１５】この方法では、まず、多重化暗号コンテンツ受信ステップにおいて、暗号化コンテンツと暗号化関連情報とが送信側で多重化された多重化暗号コンテンツが受信される。そして、多重化暗号コンテンツ分離ステップにおいて、多重化暗号コンテンツが暗号化コンテンツと暗号化関連情報とに分離され、暗号化利用制御情報復号ステップにおいて、暗号化スクランブル鍵および暗号化利用制御情報が復号される。そしてさらに、暗号化コンテンツ復号ステップにおいて、復号された利用制御情報に基づいて暗号化コンテンツが復号される。

【００１６】また、請求項５記載のコンテンツ利用制御受信方法は、経過時間に伴って変更されるスクランブル鍵によりデジタル放送におけるコンテンツを暗号化した暗号化コンテンツと、前記コンテンツ毎に設けられたコンテンツ鍵により少なくとも当該暗号化コンテンツの再生順序を制御する再生順序制御情報および前記スクランブル鍵を含む関連情報を暗号化した暗号化関連情報と、前記コンテンツの継続時間を越えて保持されるワーク鍵により少なくとも当該暗号化コンテンツの視聴を制御する視聴制御情報および前記コンテンツ鍵を含む当該コンテンツ鍵に関するコンテンツ鍵関連情報を暗号化した暗号化コンテンツ鍵関連情報と、送信側に共通に備えられるマスター鍵により少なくとも前記ワーク鍵を含むワーク鍵に関するワーク鍵関連情報を暗号化した暗号化ワーク鍵関連情報とを送信側で多重化した多重化暗号コンテンツを受信するコンテンツ利用制御受信方法であって、前記多重化暗号コンテンツを受信する多重化暗号コンテンツ受信ステップと、この多重化暗号コンテンツ受信ステップで受信した多重化暗号コンテンツを、前記暗号化コンテンツ、前記暗号化関連情報、前記暗号化コンテンツ鍵関連情報、前記暗号化ワーク鍵関連情報に分離する多重化暗号コンテンツ分離ステップと、この多重化暗号コンテンツ分離ステップで分離された暗号化ワーク鍵関連情報を前記マスター鍵で復号しワーク鍵を得る暗号化ワーク鍵関連情報復号ステップと、この暗号化ワーク鍵関連情報復号ステップで得られたワーク鍵で暗号化コンテンツ鍵関連情報に含まれている暗号化コンテンツ鍵および暗号化視聴制御情報を復号しコンテンツ鍵および視聴制御情報を得る暗号化コンテンツ鍵関連情報復号ステップと、この暗号化コンテンツ鍵関連情報復号ステップで復号された視聴制御情報に基づいて、前記暗号化関連情報に含まれている暗号化スクランブル鍵および暗号化再生順序制御情報を復号しスクランブル鍵および再生順序制御情報を得る暗号化関連情報復号ステップと、この暗号化関連情報復号ステップで復号された再生順序制御情報に基づいて、復号されたスクランブル鍵により前記暗号化コンテンツを復号する暗号化コンテンツ復号ステップと、を含むことを特徴とする。

【００１７】この方法では、まず、多重化暗号コンテンツ受信ステップにおいて、暗号化コンテンツ、暗号化関連情報、暗号化コンテンツ鍵関連情報、暗号化ワーク鍵関連情報が送信側で多重化された多重化暗号コンテンツが受信される。そして、多重化暗号コンテンツ分離ステップにおいて、これらが分離される。そしてまた、ここで分離された暗号化ワーク鍵関連情報がマスター鍵で復号されワーク鍵が得られ、暗号化コンテンツ鍵関連情報復号ステップにおいて、得られたワーク鍵で暗号化コンテンツ鍵および暗号化視聴制御情報が復号され、コンテンツ鍵および視聴制御情報が得られる。この視聴制御情報に基づいて、暗号化関連情報復号ステップにおいて、暗号化スクランブル鍵および暗号化再生順序制御情報が復号され、この再生順序制御情報に基づいて、暗号化コンテンツ復号ステップにおいて、スクランブル鍵で暗号化コンテンツが復号される。

【００１８】或いはまた、請求項６記載のコンテンツ利用制御送信装置は、デジタル放送におけるコンテンツを暗号化した暗号化コンテンツと、受信側で当該暗号化コンテンツの利用を制御する利用制御情報とを送信するコンテンツ利用制御送信装置であって、経過時間に伴って変更されるスクランブル鍵を生成するスクランブル鍵生成手段と、共通鍵暗号化方式に供される共通鍵を記憶する記憶手段と、前記スクランブル鍵により、前記コンテンツを暗号化して暗号化コンテンツとするコンテンツ暗号化手段と、前記共通鍵により、少なくとも前記利用制御情報および前記スクランブル鍵を含む関連情報を暗号化し暗号化関連情報とする関連情報暗号化手段と、前記暗号化コンテンツ、前記暗号化関連情報を多重化し多重暗号コンテンツとする多重化手段と、この多重化手段で多重化された多重化暗号コンテンツを送信する多重化暗号コンテンツ送信手段と、を備えることを特徴とする。

【００１９】かかる構成によれば、まず、スクランブル鍵生成手段で生成されたスクランブル鍵を用いて、コンテンツ暗号化手段でコンテンツが暗号化され暗号化コンテンツとされる。一方、関連情報暗号化手段で、スクランブル鍵を含む関連情報と利用制御情報とが、記憶手段に記憶されている共通鍵によって暗号化され暗号化関連情報とされる。そして、これらが多重化手段で多重化され多重化暗号コンテンツとされ、多重化暗号コンテンツ送信手段で送信される。

【００２０】また、請求項７記載のコンテンツ利用制御送信装置は、請求項６に記載のコンテンツ利用制御送信装置において、前記利用制御情報は、当該暗号化コンテンツの再生順序を制御する再生順序制御情報と、当該暗号化コンテンツの視聴を制御する視聴制御情報との少なくとも一方の情報を含んでいることを特徴とする。

【００２１】かかる構成によれば、利用制御情報が再生順序制御情報と視聴制御情報との少なくとも一方の情報を含んでいるので、受信側でコンテンツを利用するときに、この情報に従って、送信側の意図するようにコンテンツの利用制御がなされる。

【００２２】また、請求項８記載のコンテンツ利用制御送信装置は、デジタル放送におけるコンテンツを暗号化した暗号化コンテンツと、受信側で当該暗号化コンテンツの再生順序を制御する再生順序制御情報および当該暗号化コンテンツの視聴を制御する視聴制御情報と、を送信するコンテンツ利用制御送信装置であって、経過時間に伴って変更されるスクランブル鍵を生成するスクランブル鍵生成手段と、前記コンテンツ毎に設けられたコンテンツ鍵、前記コンテンツの継続時間を越えて保持されるワーク鍵、受信側に共通に備えられるマスター鍵を記憶する記憶手段と、前記スクランブル鍵により、前記コンテンツを暗号化して暗号化コンテンツとするコンテンツ暗号化手段と、前記コンテンツ鍵により、少なくとも前記再生順序制御情報および前記スクランブル鍵を含む関連情報を暗号化し暗号化関連情報とする関連情報暗号化手段と、前記ワーク鍵により、少なくとも前記視聴制御情報および前記コンテンツ鍵を含む当該コンテンツ鍵に関するコンテンツ鍵関連情報を暗号化し暗号化コンテンツ鍵関連情報とするコンテンツ鍵関連情報暗号化手段と、前記マスター鍵により、少なくとも前記ワーク鍵を含むワーク鍵に関するワーク鍵関連情報を暗号化し暗号化ワーク鍵関連情報とするワーク鍵関連情報暗号化手段と、前記暗号化コンテンツ、前記暗号化関連情報、前記暗号化コンテンツ鍵関連情報、前記暗号化ワーク鍵関連情報を多重化した多重化暗号コンテンツとする多重化手段と、この多重化手段で多重化された多重化暗号コンテンツを送信する多重化暗号コンテンツ送信手段と、を備えることを特徴とする。

【００２３】かかる構成によれば、まず、スクランブル鍵生成手段で生成されたスクランブル鍵を用いて、コンテンツ暗号化手段でコンテンツが暗号化され暗号化コンテンツとされる。一方、関連情報暗号化手段で、記憶手段に記憶されているコンテンツ鍵によって、少なくとも再生順序制御情報およびスクランブル鍵を含む関連情報が暗号化し暗号化関連情報とされる。また、コンテンツ鍵関連情報暗号化手段で、記憶手段に記憶されているワーク鍵によって、少なくとも視聴制御情報およびコンテンツ鍵を含む当該コンテンツ鍵に関するコンテンツ鍵関連情報が暗号化され暗号化コンテンツ鍵関連情報とされる。さらに、ワーク鍵関連情報暗号化手段で、マスター鍵によって、少なくともワーク鍵を含むワーク鍵に関するワーク鍵関連情報が暗号化され暗号化ワーク鍵関連情報とされる。そして、多重化手段で、これらが多重化暗号コンテンツとされ、多重化暗号コンテンツ送信手段で送信される。

【００２４】さらに、請求項９記載のコンテンツ利用制御受信装置は、経過時間に伴って変更されるスクランブル鍵によりデジタル放送におけるコンテンツを暗号化した暗号化コンテンツと、共通鍵暗号化方式に供される共通鍵により、少なくとも当該暗号化コンテンツの利用を制御する利用制御情報および前記スクランブル鍵を含む関連情報を暗号化した暗号化関連情報とを送信側で多重化した多重化暗号コンテンツを受信するコンテンツ利用制御受信装置であって、前記多重化暗号コンテンツを受信する多重化暗号コンテンツ受信手段と、この多重化暗号コンテンツ受信手段で受信した多重化暗号コンテンツを、前記暗号化コンテンツ、前記暗号化関連情報に分離する多重化暗号コンテンツ分離手段と、この多重化暗号コンテンツ分離手段で分離された暗号化関連情報に含まれている暗号化スクランブル鍵および暗号化利用制御情報を、前記共通鍵により復号する暗号化利用制御情報復号手段と、この暗号化利用制御情報復号手段で復号された利用制御情報に基づいて、復号されたスクランブル鍵により前記暗号化コンテンツを復号する暗号化コンテンツ復号手段と、を備えることを特徴とする。

【００２５】かかる構成によれば、まず、多重化暗号コンテンツ受信手段で、暗号化コンテンツと暗号化関連情報とが送信側で多重化された多重化暗号コンテンツが受信される。そして、多重化暗号コンテンツ分離手段で、多重化暗号コンテンツが暗号化コンテンツと暗号化関連情報とに分離され、暗号化利用制御情報復号手段で、暗号化スクランブル鍵および暗号化利用制御情報が復号される。そしてさらに、暗号化コンテンツ復号手段で、復号された利用制御情報に基づいて暗号化コンテンツが復号される。

【００２６】また、請求項１０記載のコンテンツ利用制御受信装置は、経過時間に伴って変更されるスクランブル鍵によりデジタル放送におけるコンテンツを暗号化した暗号化コンテンツと、前記コンテンツ毎に設けられたコンテンツ鍵により少なくとも当該暗号化コンテンツの再生順序を制御する再生順序制御情報および前記スクランブル鍵を含む関連情報を暗号化した暗号化関連情報と、前記コンテンツの継続時間を越えて保持されるワーク鍵により少なくとも当該暗号化コンテンツの視聴を制御する視聴制御情報および前記コンテンツ鍵を含む当該コンテンツ鍵に関するコンテンツ鍵関連情報を暗号化した暗号化コンテンツ鍵関連情報と、送信側に共通に備えられるマスター鍵により少なくとも前記ワーク鍵を含むワーク鍵に関するワーク鍵関連情報を暗号化した暗号化

ワーク鍵関連情報とを送信側で多重化した多重化暗号コンテンツを受信するコンテンツ利用制御受信装置であって、前記多重化暗号コンテンツを受信する多重化暗号コンテンツ受信手段と、この多重化暗号コンテンツ受信手段で受信した多重化暗号コンテンツを、前記暗号化コンテンツ、前記暗号化関連情報、前記暗号化コンテンツ鍵関連情報、前記暗号化ワーク鍵関連情報に分離する多重化暗号コンテンツ分離手段と、この多重化暗号コンテンツ分離手段で分離された暗号化ワーク鍵関連情報を前記マスター鍵で復号しワーク鍵を得る暗号化ワーク鍵関連情報復号手段と、この暗号化ワーク鍵関連情報復号手段で得られたワーク鍵で暗号化コンテンツ鍵関連情報に含まれている暗号化コンテンツ鍵および暗号化視聴制御情報を復号しコンテンツ鍵および視聴制御情報を得る暗号化コンテンツ鍵関連情報復号手段と、この暗号化コンテンツ鍵関連情報復号手段で復号された視聴制御情報に基づいて、前記暗号化関連情報に含まれている暗号化スクランブル鍵および暗号化再生順序制御情報を復号しスクランブル鍵および再生順序制御情報を得る暗号化関連情報復号手段と、この暗号化関連情報復号手段で復号された再生順序制御情報に基づいて、復号されたスクランブル鍵により前記暗号化コンテンツを復号する暗号化コンテンツ復号手段と、を備えることを特徴とする。

【００２７】かかる構成によれば、まず、多重化暗号コンテンツ受信手段で、暗号化コンテンツ、暗号化関連情報、暗号化コンテンツ鍵関連情報、暗号化ワーク鍵関連情報が送信側で多重化された多重化暗号コンテンツが受信される。そして、多重化暗号コンテンツ分離手段で、これらが分離される。そしてまた、ここで分離された暗号化ワーク鍵関連情報がマスター鍵で復号されワーク鍵が得られ、暗号化コンテンツ鍵関連情報復号手段で、得られたワーク鍵で暗号化コンテンツ鍵および暗号化視聴制御情報が復号され、コンテンツ鍵および視聴制御情報が得られる。この視聴制御情報に基づいて、暗号化関連情報復号手段で、暗号化スクランブル鍵および暗号化再生順序制御情報が復号され、この再生順序制御情報に基づいて、暗号化コンテンツ復号手段で、スクランブル鍵で暗号化コンテンツが復号される。

【００２８】さらにまた、請求項１１記載のコンテンツ利用制御送信プログラムは、デジタル放送におけるコンテンツを暗号化した暗号化コンテンツと、受信側で当該暗号化コンテンツの利用を制御する利用制御情報とを送信するコンテンツ利用制御送信装置を、以下に示す手段として機能させることを特徴とする。コンテンツ利用制御送信装置を機能させる手段は、経過時間に伴って変更されるスクランブル鍵を生成するスクランブル鍵生成手段、共通鍵暗号化方式に供される共通鍵を記憶する記憶手段、前記スクランブル鍵により、前記コンテンツを暗号化して暗号化コンテンツとするコンテンツ暗号化手段、前記共通鍵により、少なくとも前記利用制御情報および前記スクランブル鍵を含む関連情報を暗号化し暗号化関連情報とする関連情報暗号化手段、前記暗号化コンテンツ、前記暗号化関連情報を多重化し多重暗号コンテンツとする多重化手段、この多重化手段で多重化された多重化暗号コンテンツを送信する多重化暗号コンテンツ送信手段、である。

【００２９】かかる構成によれば、まず、スクランブル鍵生成手段で生成されたスクランブル鍵を用いて、コンテンツ暗号化手段でコンテンツが暗号化され暗号化コンテンツとされる。一方、関連情報暗号化手段で、スクランブル鍵を含む関連情報と利用制御情報とが、記憶手段に記憶されている共通鍵によって暗号化され暗号化関連情報とされる。そして、これらが多重化手段で多重化され多重化暗号コンテンツとされ、多重化暗号コンテンツ送信手段で送信される。

【００３０】また、請求項１２記載のコンテンツ利用制御送信プログラムは、請求項１１に記載のコンテンツ利用制御送信プログラムにおいて、前記利用制御情報は、当該暗号化コンテンツの再生順序を制御する再生順序制御情報と、当該暗号化コンテンツの視聴を制御する視聴制御情報との少なくとも一方の情報を含んでいることを特徴とする。

【００３１】かかる構成によれば、利用制御情報が再生順序制御情報と視聴制御情報との少なくとも一方の情報を含んでいるので、受信側でコンテンツを利用するときに、この情報に従って、送信側の意図するようにコンテンツの利用制御がなされる。

【００３２】また、請求項１３記載のコンテンツ利用制御送信プログラムは、デジタル放送におけるコンテンツを暗号化した暗号化コンテンツと、受信側で当該暗号化コンテンツの再生順序を制御する再生順序制御情報および当該暗号化コンテンツの視聴を制御する視聴制御情報と、を送信するコンテンツ利用制御送信装置を、以下に示す手段として機能させることを特徴とする。コンテンツ利用制御装置を機能させる手段は、経過時間に伴って変更されるスクランブル鍵を生成するスクランブル鍵生成手段、前記コンテンツ毎に設けられたコンテンツ鍵、前記コンテンツの継続時間を越えて保持されるワーク鍵、受信側に共通に備えられるマスター鍵を記憶する記憶手段、前記スクランブル鍵により、前記コンテンツを暗号化して暗号化コンテンツとするコンテンツ暗号化手段、前記コンテンツ鍵により、少なくとも前記再生順序制御情報および前記スクランブル鍵を含む関連情報を暗号化し暗号化関連情報とする関連情報暗号化手段、前記ワーク鍵により、少なくとも前記視聴制御情報および前記コンテンツ鍵を含む当該コンテンツ鍵に関するコンテンツ鍵関連情報を暗号化し暗号化コンテンツ鍵関連情報とするコンテンツ鍵関連情報暗号化手段、前記マスター鍵により、少なくとも前記ワーク鍵を含むワーク鍵に関するワーク鍵関連情報を暗号化し暗号化ワーク鍵関連情

報とするワーク鍵関連情報暗号化手段、前記暗号化コンテンツ、前記暗号化関連情報、前記暗号化コンテンツ鍵関連情報、前記暗号化ワーク鍵関連情報を多重化した多重化暗号コンテンツとする多重化手段、この多重化手段で多重化された多重化暗号コンテンツを送信する多重化暗号コンテンツ送信手段、である。

【００３３】かかる構成によれば、まず、スクランブル鍵生成手段で生成されたスクランブル鍵を用いて、コンテンツ暗号化手段でコンテンツが暗号化され暗号化コンテンツとされる。一方、関連情報暗号化手段で、記憶手段に記憶されているコンテンツ鍵によって、少なくとも再生順序制御情報およびスクランブル鍵を含む関連情報が暗号化し暗号化関連情報とされる。また、コンテンツ鍵関連情報暗号化手段で、記憶手段に記憶されているワーク鍵によって、少なくとも視聴制御情報およびコンテンツ鍵を含む当該コンテンツ鍵に関するコンテンツ鍵関連情報が暗号化され暗号化コンテンツ鍵関連情報とされる。さらに、ワーク鍵関連情報暗号化手段で、マスター鍵によって、少なくともワーク鍵を含むワーク鍵に関するワーク鍵関連情報が暗号化され暗号化ワーク鍵関連情報とされる。そして、多重化手段で、これらが多重化暗号コンテンツとされ、多重化暗号コンテンツ送信手段で送信される。

【００３４】さらに、請求項１４記載のコンテンツ利用制御受信プログラムは、経過時間に伴って変更されるスクランブル鍵によりデジタル放送におけるコンテンツを暗号化した暗号化コンテンツと、共通鍵暗号化方式に供される共通鍵により、少なくとも当該暗号化コンテンツの利用を制御する利用制御情報および前記スクランブル鍵を含む関連情報を暗号化した暗号化関連情報とを送信側で多重化した多重化暗号コンテンツを受信するコンテンツ利用制御受信装置を、以下に示す手段として機能させることを特徴とする。コンテンツ利用制御受信装置を機能させる手段は、前記多重化暗号コンテンツを受信する多重化暗号コンテンツ受信手段、この多重化暗号コンテンツ受信手段で受信した多重化暗号コンテンツを、前記暗号化コンテンツ、前記暗号化関連情報に分離する多重化暗号コンテンツ分離手段、この多重化暗号コンテンツ分離手段で分離された暗号化関連情報に含まれている暗号化スクランブル鍵および暗号化利用制御情報を、前記共通鍵により復号する暗号化利用制御情報復号手段、この暗号化利用制御情報復号手段で復号された利用制御情報に基づいて、復号されたスクランブル鍵により前記暗号化コンテンツを復号する暗号化コンテンツ復号手段、である。

【００３５】かかる構成によれば、まず、多重化暗号コンテンツ受信手段で、暗号化コンテンツと暗号化関連情報とが送信側で多重化された多重化暗号コンテンツが受信される。そして、多重化暗号コンテンツ分離手段で、多重化暗号コンテンツが暗号化コンテンツと暗号化関連情報とに分離され、暗号化利用制御情報復号手段で、暗号化スクランブル鍵および暗号化利用制御情報が復号される。そしてさらに、暗号化コンテンツ復号手段で、復号された利用制御情報に基づいて暗号化コンテンツが復号される。

【００３６】また、請求項１５記載のコンテンツ利用制御受信プログラムは、経過時間に伴って変更されるスクランブル鍵によりデジタル放送におけるコンテンツを暗号化した暗号化コンテンツと、前記コンテンツ毎に設けられたコンテンツ鍵により少なくとも当該暗号化コンテンツの再生順序を制御する再生順序制御情報および前記スクランブル鍵を含む関連情報を暗号化した暗号化関連情報と、前記コンテンツの継続時間を越えて保持されるワーク鍵により少なくとも当該暗号化コンテンツの視聴を制御する視聴制御情報および前記コンテンツ鍵を含む当該コンテンツ鍵に関するコンテンツ鍵関連情報を暗号化した暗号化コンテンツ鍵関連情報と、送信側に共通に備えられるマスター鍵により少なくとも前記ワーク鍵を含むワーク鍵に関するワーク鍵関連情報を暗号化した暗号化ワーク鍵関連情報とを送信側で多重化した多重化暗号コンテンツを受信するコンテンツ利用制御受信装置を、以下に示す手段として機能させることを特徴とする。コンテンツ利用制御受信装置を機能させる手段は、前記多重化暗号コンテンツを受信する多重化暗号コンテンツ受信手段、この多重化暗号コンテンツ受信手段で受信した多重化暗号コンテンツを、前記暗号化コンテンツ、前記暗号化関連情報、前記暗号化コンテンツ鍵関連情報、前記暗号化ワーク鍵関連情報に分離する多重化暗号コンテンツ分離手段、この多重化暗号コンテンツ分離手段で分離された暗号化ワーク鍵関連情報を前記マスター鍵で復号しワーク鍵を得る暗号化ワーク鍵関連情報復号手段、この暗号化ワーク鍵関連情報復号手段で得られたワーク鍵で暗号化コンテンツ鍵関連情報に含まれている暗号化コンテンツ鍵および暗号化視聴制御情報を復号しコンテンツ鍵および視聴制御情報を得る暗号化コンテンツ鍵関連情報復号手段、この暗号化コンテンツ鍵関連情報復号手段で復号された視聴制御情報に基づいて、前記暗号化関連情報に含まれている暗号化スクランブル鍵および暗号化再生順序制御情報を復号しスクランブル鍵および再生順序制御情報を得る暗号化関連情報復号手段、この暗号化関連情報復号手段で復号された再生順序制御情報に基づいて、復号されたスクランブル鍵により前記暗号化コンテンツを復号する暗号化コンテンツ復号手段、である。

【００３７】かかる構成によれば、まず、多重化暗号コンテンツ受信手段で、暗号化コンテンツ、暗号化関連情報、暗号化コンテンツ鍵関連情報、暗号化ワーク鍵関連情報が送信側で多重化された多重化暗号コンテンツが受信される。そして、多重化暗号コンテンツ分離手段で、これらが分離される。そしてまた、ここで分離された暗

号化ワーク鍵関連情報がマスター鍵で復号されワーク鍵が得られ、暗号化コンテンツ鍵関連情報復号手段で、得られたワーク鍵で暗号化コンテンツ鍵および暗号化視聴制御情報が復号され、コンテンツ鍵および視聴制御情報が得られる。この視聴制御情報に基づいて、暗号化関連情報復号手段で、暗号化スクランブル鍵および暗号化再生順序制御情報が復号され、この再生順序制御情報に基づいて、暗号化コンテンツ復号手段で、スクランブル鍵で暗号化コンテンツが復号される。

【００３８】

【発明の実施の形態】以下、本発明の一実施形態を図面に基づいて詳細に説明する。

（コンテンツ利用制御システム（コンテンツ利用制御送信装置およびコンテンツ利用制御受信装置））図１にコンテンツ利用制御システムのブロック図を示す。この図１に示すように、コンテンツ利用制御システム１は、コンテンツ利用制御送信装置３とコンテンツ利用制御受信装置５とを備えて構成されている。

【００３９】コンテンツ利用制御システム１は、デジタル放送におけるコンテンツを暗号化して受信側で当該暗号化したコンテンツの利用（再生、編集等）を制御（制限）する情報（利用制御情報）と共に送信することで、受信側でのコンテンツの利用を制御可能にするシステムである。

【００４０】（コンテンツ利用制御送信装置の構成）まず、コンテンツ利用制御送信装置３について説明する。コンテンツ利用制御送信装置３は、コンテンツスクランブル部７と、多重化部９と、記憶部１１とを備えて構成されている。コンテンツ利用制御送信装置３は、映像・音声データからなるコンテンツを暗号化して、受信側のコンテンツ利用制御受信装置５に送信するものであって、受信側と共通に備えられるマスター鍵を利用して（このため、共通鍵暗号化方式とされる）当該コンテンツを暗号化し送信するものである。

【００４１】コンテンツスクランブル部７は、まず、図示を省略したスクランブル鍵生成部で生成されたスクランブル鍵Ｋｓを用いて、送信するコンテンツを暗号化し暗号化コンテンツとする（暗号化器７ａ）。次に、記憶部１１に記憶されているコンテンツ鍵Ｋｃを用いて、少なくともスクランブル鍵Ｋｓおよび再生手順番号（再生順序制御情報：利用制御情報の１つ）を含む関連情報を暗号化し暗号化関連情報とする（暗号化器７ｂ）。つまり、暗号化されたスクランブル鍵Ｋｓは、ＭＰＥＧ－２多重化方式のセクション形式でパケット化される。このパケット化の具体的な方式の例として、ＡＲＩＢの限定受信方式規格（ＳＴＤ－Ｂ２５）に記載されたＥＣＭ（Ｅｎｔｉｔｌｅｍｅｎｔ　Ｃｏｎｔｒｏｌ　Ｍｅｓｓａｇｅ）形式が利用でき、同規格と同様な方式でパケット化し送出することができる。

【００４２】また、コンテンツスクランブル部７は、記憶部１１に記憶されているワーク鍵Ｋｗを用いて、少なくともコンテンツ鍵Ｋｃおよび視聴制御フラグ（視聴制御情報：利用制御情報の１つ）を含む当該コンテンツ鍵に関するコンテンツ鍵関連情報を暗号化し暗号化コンテンツ鍵関連情報とする（暗号化器７ｃ）。さらに、記憶部１１に記憶されているマスター鍵Ｋｍを用いて、少なくともワーク鍵Ｋｗを含むワーク鍵Ｋｗに関するワーク鍵関連情報を暗号化し暗号化ワーク鍵関連情報とする（暗号化器７ｄ）。

【００４３】なお、コンテンツをコンテンツ利用制御受信装置５でリアルタイムに視聴させる場合には、コンテンツ鍵Ｋｃ（暗号化コンテンツ鍵Ｋｃ）の送出が、当該コンテンツを送出する所定時間前から開始され、コンテンツが送出されている間、コンテンツ鍵Ｋｃが所定時間間隔で繰り返し送出され、コンテンツ送出終了後、コンテンツ鍵Ｋｃの送出も終了される。一方、コンテンツをコンテンツ利用制御受信装置５の記憶部（後記する）に記憶後、記憶したコンテンツを再生させて視聴する場合には、記憶部にスクランブルしたままのコンテンツ（暗号化コンテンツ）を記憶させておき、当該コンテンツの視聴を許可するとき（送信側で制御）に、当該コンテンツに対応するコンテンツ鍵Ｋｃが送出される。

【００４４】また、コンテンツ利用制御送信装置３のコンテンツスクランブル部７と請求項に記載した構成との対応関係を補足すると、コンテンツスクランブル部７（７ａ）がコンテンツ暗号化手段に、暗号化器７ｂが関連情報暗号化手段に、暗号化器７ｃがコンテンツ鍵関連情報暗号化手段に、暗号化器７ｄがワーク鍵関連情報暗号化手段に相当するものである。

【００４５】多重化部９は、コンテンツスクランブル部７で暗号化された暗号化コンテンツと、暗号化関連情報と、暗号化コンテンツ鍵関連情報と、暗号化ワーク鍵関連情報とをトランスポートストリームとして多重化して多重化暗号コンテンツを生成し、受信側に送出するものである。なお、この多重化部９が請求項に記載した多重化手段と多重化暗号コンテンツ送信手段に相当するものである。

【００４６】記憶部１１は、コンテンツ鍵Ｋｃ、ワーク鍵Ｋｗ、マスター鍵Ｋｍを記憶しておくものであり、それぞれ、コンテンツ鍵Ｋｃデータベース、ワーク鍵Ｋｗデータベース、マスター鍵Ｋｍデータベースといった形式で記憶（格納）されている。

【００４７】ここで、各暗号鍵、利用制御情報について補足説明しておく。スクランブル鍵Ｋｓは、経過時間（数秒単位）に伴って変更される暗号鍵であり、コンテンツ鍵Ｋｃは、コンテンツ毎に設定される暗号鍵である。また、ワーク鍵Ｋｗは、コンテンツの継続時間を越えて保持される暗号鍵であり、マスター鍵Ｋｍは、コンテンツ利用制御受信装置５に備えられている送受信間で共通の暗号鍵である。そして、このマスター鍵Ｋｍは、

コンテンツ利用制御受信装置５（後記するセキュリティモジュール）各々に割り当てられた固有の鍵である。なお、このマスター鍵Ｋｍは、予めセキュリティモジュール内に書き込まれて、受信側（コンテンツ利用制御受信装置５に付属させて）に配布されている。

【００４８】そして、視聴制御フラグ（視聴制御情報）は、コンテンツの視聴をフラグのオンオフで制御するもので、フラグがオンの場合、受信側で暗号化スクランブルが復号後、再生手順番号に基づいてコンテンツの視聴が決定される。フラグがオフの場合、受信側で即座に暗号化スクランブル鍵が復号されてコンテンツの視聴が許可される。さらに、再生手順番号（再生順序制御情報）は、コンテンツの視聴順序を制御する情報であり、詳細は後記する。

【００４９】（コンテンツ利用制御受信装置の構成）次に、コンテンツ利用制御受信装置５について説明する。コンテンツ利用制御受信装置５は、分離部１３と、コンテンツデスクランブル部１５と、記憶部１７とを備えて構成されている。コンテンツ利用制御受信装置５は、送信側のコンテンツ利用制御送信装置３で暗号化され、多重化された多重化暗号コンテンツを受信し、この多重化暗号コンテンツに含まれている利用制御情報（視聴制御フラグ、再生手順番号）に従って、多重化暗号コンテンツを復号し、コンテンツを視聴可能にするものである。

【００５０】分離部１３は、送信側のコンテンツ利用制御送信装置３から送信された多重化暗号コンテンツを受信すると共に、受信した多重化暗号コンテンツを、暗号化コンテンツ、暗号化関連情報、暗号化コンテンツ鍵関連情報、暗号化ワーク鍵関連情報に分離するものである。この分離部１３が請求項に記載した多重化暗号コンテンツ受信手段と多重化暗号コンテンツ分離手段とに相当するものである。

【００５１】コンテンツデスクランブル部１５は、４つの復号器（後記するセキュリティモジュールＳＭ）を備えて構成されており、分離部１３で分離された暗号化コンテンツ、暗号化関連情報、暗号化コンテンツ鍵関連情報、暗号化ワーク鍵関連情報を復号するものであって、まず、暗号化ワーク鍵関連情報がマスター鍵により復号されワーク鍵が得られる（復号器１５ａ）。

【００５２】そして、このワーク鍵により暗号化コンテンツ鍵関連情報が復号されコンテンツ鍵および視聴制御フラグが得られ（復号器１５ｂ）、この視聴制御フラグ（オンｏｒオフ）に基づいて、コンテンツ鍵により暗号化関連情報が復号され、スクランブル鍵のみ、または、スクランブル鍵および再生手順番号が得られる（復号器１５ｃ）。

【００５３】さらに、この再生手順番号に基づいて、スクランブル鍵により暗号化コンテンツが復号され、コンテンツが得られる（コンテンツデスクランブル部１５（復号器１５ｄ））。このコンテンツデスクランブル部１５が、請求項に記載した多重暗号コンテンツ復号手段に相当するものである。記憶部１７は、コンテンツ利用制御受信装置５本体に一体的に備えられているメモリ部１７ａと、記憶媒体に情報を記憶させる記憶媒体取扱手段１７ｂとを備えて構成されている。

【００５４】また、コンテンツ利用制御受信装置５には、この図１において図示を省略したセキュリティモジュールＳＭ１が備えられている。このセキュリティモジュールＳＭ１は、少なくとも復号器１５ａ～１５ｃを備え、マスター鍵Ｋｍが保持されるものであって、外部より読み出し不可能なＩＣカード等から構成されている。またこのセキュリティモジュールＳＭ１には、図示を省略した記憶部Ｎが備えられており、この記憶部Ｎは、再生手順番号の数値（利用制御情報の１つ）を記憶するカウンタに相当するものである。なお、この記憶部Ｎに記憶される再生手順番号の数値は、初期値として１が記憶されており、コンテンツ鍵関連情報に含まれるコンテンツＩＤおよびコンテンツ鍵Ｋｃが変更されるたびに数値の再設定（初期値１に設定）が行われる。

【００５５】（ワーク鍵Ｋｗの共有化について）ここで、ある複数のコンテンツ利用制御受信装置５において、ワーク鍵Ｋｗを共有させたい場合を想定して説明する。まず、送信側のコンテンツ利用制御送信装置３は、該当するコンテンツ利用制御受信装置５のマスター鍵Ｋｍを、記憶部１１のマスター鍵Ｋｍデータベースより読み出し、このマスター鍵Ｋｍによりワーク鍵Ｋｗを共通鍵暗号化方式の暗号化器７ｄで暗号化する。この暗号化されたワーク鍵Ｋｗ（暗号化ワーク鍵Ｋｗ）を含む関連情報を、例えば、ＭＰＥＧ－２多重化方式のセクション形式でパケット化し、個別情報として、多重化部９で暗号化した暗号化コンテンツと併せてトランスポートストリームとして多重化する。

【００５６】このパケット化の例として、ＡＲＩＢの限定受信方式規格（ＳＴＤ－Ｂ２５）に記載されたＥＭＭ（Ｅｎｔｉｔｌｅｍｅｎｔ　Ｍａｎａｇｅｍｅｎｔ　Ｍｅｓｓａｇｅ）形式が利用可能である。そして、受信側のコンテンツ利用制御受信装置５では、分離部１３で受信したＭＰＥＧ－２トランスポートストリームから、ＥＭＭを取り出し、マスター鍵Ｋｍを用いて、復号器１５ａで復号し、ワーク鍵Ｋｗを得る。

【００５７】この動作を、各コンテンツ利用制御受信装置５に対して繰り返し実行し、これにより、ワーク鍵Ｋｗを送受信間で共有させることができる。また、得られたワーク鍵Ｋｗは、セキュリティモジュールＳＭ（図１には図示せず）に保存される。そして、複数のコンテンツ利用制御受信装置５間で共有化された当該ワーク鍵Ｋｗは、ワーク鍵Ｋｗ自体の安全性を維持するために、例えば１ヶ月や１年といった単位で更新される。また、このワーク鍵Ｋｗは放送帯域の空いた帯域を利用して、コンテンツとは独立に順次送信される。

【００５８】（ファイルフォーマットの例）次に、送信側のコンテンツ利用制御送信装置３から送信されるファイルのフォーマット例を図２を参照して説明する。コンテンツ利用制御送信装置３から送信されるファイルのフォーマットには、スクランブル鍵関連情報Ｓ（共通情報Ｓ）、コンテンツ鍵関連情報Ｃ（共通情報Ｃ）、ワーク鍵鍵関連情報Ｗ（個別情報Ｗ）の３種類がある。

【００５９】スクランブル鍵関連情報Ｓ（共通情報Ｓ）は、スクランブル鍵の送出に用いられる番組情報であり、事業者ＩＤ、コンテンツＩＤ、スクランブル鍵Ｋｓ、再生手順番号等から構成されている。事業者ＩＤは放送事業者に割り当てられた識別子であり、コンテンツＩＤは、コンテンツ毎にユニークに、或いは、所定の条件（例えば、再放送番組を同一ＩＤとするか別のＩＤとするか等の条件）に基づいて、割り当てられた識別子である。そして、スクランブル鍵Ｋｓは、コンテンツＩＤに対応するコンテンツ鍵Ｋｃによって暗号化される。また、再生手順番号は、受信側でコンテンツの再生順序を規定するものである。

【００６０】コンテンツ鍵関連情報Ｃ（共通情報Ｃ）は、コンテンツ鍵Ｋｃの送出に用いられる共通の情報であり、事業者ＩＤ、ワーク鍵ＩＤ、コンテンツＩＤ、コンテンツ鍵Ｋｃ、有効期限、記憶場所指定、視聴制御フラグ等から構成されている。事業者ＩＤは放送事業者に割り当てられた識別子であり、ワーク鍵ＩＤはワーク鍵を識別する識別子であり、コンテンツＩＤは、コンテンツ毎にユニークに、割り当てられた識別子である。これらのうち少なくともコンテンツ鍵Ｋｃは、ワーク鍵ＩＤに対応するワーク鍵によって暗号化されている。

【００６１】また、有効期限は、コンテンツ鍵Ｋｃの有効期限を示すものであり、記憶場所指定は、受信したコンテンツ鍵をコンテンツ利用制御受信装置５のどこに記憶させるかを予め送信側で指定するものである。視聴制御フラグは、コンテンツの視聴をフラグのオンオフで制御するもので、フラグがオンの場合、受信側で暗号化スクランブルが復号後、再生手順番号に基づいてコンテンツの視聴が決定されるものである。

【００６２】ワーク鍵関連情報Ｗ（個別情報Ｗ）は、ワーク鍵Ｋｗの送出に用いられる個別情報であり、事業者ＩＤ、カードＩＤ、更新番号、有効期限、ワーク鍵ＩＤ、ワーク鍵等から構成されている。事業者ＩＤは、放送事業者或いはその特定の集合（グループ）等に割り当てられた識別子であり、カードＩＤは、セキュリティモジュールＳＭ毎に割り当てられた識別子であり、更新番号は、ワーク鍵Ｋｗのバージョンを示す番号であり、有効期限は、ワーク鍵Ｋｗの有効期限を示すものである。そして、ワーク鍵Ｋｗは、カードＩＤに対応するマスター鍵Ｋｍによって暗号化されている。

【００６３】（コンテンツ利用制御受信装置とセキュリティモジュールとの関係（構成））次に、図３を参照して、コンテンツ利用制御システム１におけるコンテンツ利用制御受信装置５とセキュリティモジュールＳＭ１との関係を説明する。コンテンツ利用制御受信装置５は、受信したストリーム（多重暗号コンテンツ）からワーク鍵Ｋｗやコンテンツ鍵Ｋｃを含む関連情報を分離するＫｗ・Ｋｃ関連情報分離部１３ａと、暗号化コンテンツを記憶する記憶部１７ａと、スクランブル鍵Ｋｓを含む関連情報を分離するＫｓ関連情報分離部１３ｂと、コンテンツをデスクランブルするコンテンツデスクランブル部１５と、コンテンツ利用制御受信装置５とセキュリティモジュールＳＭ１との通信を行うインターフェース等から構成されている。

【００６４】セキュリティモジュールＳＭ１は、マスター鍵Ｋｍを備え、４つの復号器（１９ａ～１９ｄ）と、１つの暗号化器２１と、スクランブル鍵Ｋｓを送出させる送出部２３と、この送出部２３を制御する送出制御部２５と、状況に応じて入力される複数の情報を制御するソフトウェアスイッチＳ／Ｗとを備えて構成されている。このソフトウェアスイッチＳ／Ｗに、入力される情報数は２個であり、この情報数に対応してａ１、ａ２のスイッチが備えられており、スイッチａ１がリアルタイムにコンテンツを視聴する場合、スイッチａ２が記憶再生視聴する場合に対応している。

【００６５】Ｋｗ・Ｋｃ関連情報分離部１３ａで、多重化暗号コンテンツから暗号化ワーク鍵関連情報を抽出し、この暗号化ワーク鍵関連情報に記述されているカードＩＤと、セキュリティモジュールＳＭ１（この実施の形態ではＩＣカード）のカードＩＤとが一致する場合、ワーク鍵Ｋｗ、ワーク鍵ＩＤ、更新番号、有効期限、事業者ＩＤとが含まれている暗号化ワーク鍵関連情報をセキュリティモジュールＳＭ１に入力する。セキュリティモジュールＳＭ１では、入力された暗号化されているワーク鍵Ｋｗをマスター鍵Ｋｍで復号し、ワーク鍵Ｋｗを得て（復号器１９ａ）、このワーク鍵Ｋｗは、事業者ＩＤ、更新番号、有効期限、ワーク鍵ＩＤとに対応されて、セキュリティモジュールＳＭ１内で保持される。

【００６６】一方、Ｋｗ・Ｋｃ関連情報分離部１３ａにおいて、暗号化コンテンツ鍵関連情報を抽出し、ワーク鍵ＩＤと、暗号化されているコンテンツ鍵Ｋｃ、事業者ＩＤ、有効期限、コンテンツＩＤとが含まれている暗号化コンテンツ鍵関連情報をセキュリティモジュールＳＭ１に入力する。セキュリティモジュールＳＭ１では、暗号化コンテンツ鍵関連情報をワーク鍵ＩＤに対応するワーク鍵Ｋｗを用いて復号し、コンテンツ鍵Ｋｃを得る（復号器１９ｂ）。

【００６７】（暗号化コンテンツの再生例（リアルタイム視聴））次に、図３に図示したコンテンツ利用制御受信装置５およびセキュリティモジュールＳＭ１を用いて、送信されているコンテンツ（リアルタイム）を視聴する場合について説明する。リアルタイムにコンテンツ

を視聴する場合であるので、予め、セキュリティモジュールＳＭ１のソフトウェアスイッチＳ／Ｗをａ１に切り替えておく。

【００６８】Ｋｗ・Ｋｃ関連情報分離部１３ａの出力は、Ｋｓ関連情報分離部１３ｂに入力される。Ｋｓ関連情報分離部１３ｂでは、関連情報Ｓを抽出し、コンテンツＩＤと暗号化されたスクランブル鍵Ｋｓを含む関連情報Ｓをセキュリティモジュール ＳＭ１に入力する。セキュリティモジュールＳＭ１では、関連情報Ｓをコンテンツ ＩＤに対応するコンテンツ鍵Ｋｃを用いて復号し、スクランブル鍵Ｋｓおよび再生手順番号を得る（復号器１９ｄ）。そして、得られた再生手順番号を送出制御部２５に入力し、この再生手順番号が入力された送出制御部２５は、再生手順番号に基づいて、送出部２３を制御し、復号器１９ｄで得られたスクランブル鍵Ｋｓをコンテンツ利用制御受信装置５に送出する。このスクランブル鍵Ｋｓを受信したコンテンツ利用制御受信装置５のコンテンツデスクランブル部１５は、スクランブル鍵Ｋｓを用いて暗号化コンテンツを復号し、コンテンツを出力する。

【００６９】（暗号化コンテンツの再生例（記憶再生視聴））次に、図３に図示したコンテンツ利用制御受信装置５およびセキュリティモジュールＳＭ１を用いて、記憶部１７ａに記憶したコンテンツを視聴する場合について説明する。記憶部１７ａに記憶させたコンテンツを視聴する場合であるので、予め、セキュリティモジュールＳＭ１のソフトウェアスイッチＳ／Ｗをａ２に切り替えておく。

【００７０】暗号化コンテンツはそのまま（スクランブル化されたまま）、暗号化されたスクランブル鍵を含む暗号化関連情報（関連情報Ｓ）と共に、コンテンツＩＤと対応されて、記憶部１７ａに記憶されている。一方、Ｋｗ・Ｋｃ関連情報分離部１３ａにおいて、暗号化コンテンツ鍵関連情報（コンテンツ鍵関連情報Ｃ）を抽出し、抽出した、暗号化されたコンテンツ鍵を含む暗号化コンテンツ鍵関連情報をセキュリティモジュールＳＭ１に入力する。そして、復号器１９ｂで復号されたコンテンツ鍵を、マスター鍵を用いて暗号化する（暗号化器２１）。この暗号化されたコンテンツ鍵Ｋｃをコンテンツ利用制御受信装置５に出力し、記憶部１７ａに記憶されている暗号化コンテンツと対応させて記憶する。

【００７１】そして、記憶部１７ａに記憶されているコンテンツを再生するときには、デスクランブルするコンテンツに対応する、暗号化されたコンテンツ鍵Ｋｃを記憶部１７ａから読み出して、セキュリティモジュールＳＭ１に入力する。セキュリティモジュールＳＭ１では、入力された、暗号化されているコンテンツ鍵Ｋｃをマスター鍵Ｋｍにより、復号しコンテンツ鍵Ｋｃを得る（復号器１９ｃ）。また一方、再生されたコンテンツは、Ｋｓ関連情報分離部１３ｂに入力され、暗号化関連情報（関連情報Ｓ）を抽出し、暗号化されているスクランブル鍵Ｋｓを含む暗号化関連情報（関連情報Ｓ）をセキュリティモジュールＳＭ１に入力する。

【００７２】セキュリティモジュールＳＭ１では、入力された、暗号化されているスクランブル鍵Ｋｓを含む暗号化関連情報を、復号器１９ｃで復号されたコンテンツ鍵Ｋｃで復号し、スクランブル鍵Ｋｓおよび再生手順番号を得る（復号器１９ｄ）。再生手順番号を送出制御部２５に入力し、送出制御部２５は得られた再生手順番号に基づいて、送出部２３を制御し、コンテンツ利用制御受信装置５にスクランブル鍵Ｋｓを送出する。コンテンツ利用制御受信装置５では、受信したスクランブル鍵Ｋｓを用いて、コンテンツデスクランブル部１５で暗号化コンテンツがデスクランブルされ、コンテンツが出力される。

【００７３】また、コンテンツ利用制御受信装置５にホームネットワーク等を介して、記憶装置（図示せず）が接続されている場合には、Ｋｓ関連情報分離部１３ｂに入力される前に、ストリーム（多重化暗号コンテンツの一部）が、ホームネットワーク等を介して、コンテンツ利用制御受信装置５以外の記憶装置に記憶される。

【００７４】このとき、暗号化コンテンツおよび暗号化関連情報と併せて、マスター鍵Ｋｍで暗号化した再暗号化コンテンツ鍵を記憶装置に記憶させる。暗号化コンテンツの再生時には、記憶装置で再生された信号（スクランブルされたままのコンテンツ信号）がコンテンツ利用制御受信装置５のＫｓ関連情報分離部１３ｂにホームネットワークを介して入力されると共に、コンテンツ利用制御受信装置５を介して再暗号化コンテンツ鍵がセキュリティモジュールＳＭ１に入力され、復号器１９ｃで再暗号コンテンツ鍵が復号され、復号器１９ｄでスクランブル鍵Ｋｓが得られ、コンテンツがデスクランブルされる。

【００７５】（コンテンツ利用制御受信装置に入力されるストリーム（多重化暗号コンテンツ）に対する各鍵の対応関係、再生手順番号の例）次に、図４を参照して、コンテンツ利用制御受信装置５に入力されるストリーム（多重化暗号コンテンツ：コンテンツの各シーン）に対する、スクランブル鍵Ｋｓ、コンテンツ鍵Ｋｃ、の対応関係を説明する。ここでは、コンテンツがリアルタイムに視聴される場合を想定しており、コンテンツの中身をシーンＡ、シーンＢ、シーンＣ、シーンＤ、シーンＥといった具合に時間軸方向に区切った場合について説明する。例えば、コンテンツをあるドラマであるとすると、シーンＡはドラマのプロローグに、シーンＢはＣＭに、シーンＣはドラマの中核に、シーンＤはＣＭに、シーンＥはドラマのエピローグに相当する。

【００７６】これらの各シーンＡ～Ｅをスクランブルしているスクランブル鍵Ｋｓ（Ｋｓ１１～Ｋｓ５ｎ）および再生手順番号はスクランブル鍵関連情報に含まれてい

る。シーンAの間は1秒程度の時間でスクランブル鍵Ｋｓ１１からスクランブル鍵Ｋｓ１ｎに順次変更され、スクランブル鍵Ｋｓ１１からスクランブル鍵Ｋｓ１ｎには同じ再生手順番号１が付されている。

【００７７】また、シーンBの間は、１秒程度の時間でスクランブル鍵Ｋｓ２１からスクランブル鍵Ｋｓ２ｎに順次変更され、スクランブル鍵Ｋｓ２１からスクランブル鍵Ｋｓ２ｎには複数の再生手順番号２、３、４、５が付されている。シーンCの間は１秒程度の時間でスクランブル鍵Ｋｓ３１からスクランブル鍵Ｋｓ３ｎに順次変更され、スクランブル鍵Ｋｓ３１からスクランブル鍵Ｋｓ３ｎには同じ再生手順番号６が付されている。

【００７８】さらに、シーンDの間は、１秒程度の時間でスクランブル鍵Ｋｓ４１からスクランブル鍵Ｋｓ４ｎに順次変更され、スクランブル鍵Ｋｓ４１からスクランブル鍵Ｋｓ４ｎには複数の再生手順番号７、８、９が付されている。シーンEの間は１秒程度の時間でスクランブル鍵Ｋｓ５１からスクランブル鍵Ｋｓ５ｎに順次変更され、スクランブル鍵Ｋｓ５１からスクランブル鍵Ｋｓ５ｎには同じ再生手順番号１０が付されている。

【００７９】なお、多重化暗号コンテンツには、コンテンツ鍵関連情報Ｃ１（暗号化されている）が含まれており、このコンテンツ鍵関連情報Ｃ１には、コンテンツ鍵Ｋｃ、視聴制御フラグ（オン）が含まれている。このコンテンツ鍵Ｋｃはコンテンツの各シーンすなわちシーンAからシーンDまで、同一のものが用いられる。また、視聴制御フラグがオンであれば、再生手順番号に基づいてコンテンツ利用制御受信装置５にスクランブル鍵Ｋｓが送出され、視聴制御フラグがオフであれば、再生手順番号に拘わらずコンテンツ利用制御受信装置５にスクランブル鍵Ｋｓが送出される。

【００８０】（コンテンツの視聴制御（利用制御）の例１）ここで、図３、図４を参照して、コンテンツに付されている再生手順番号に基づいたコンテンツ（シーンA～E）の視聴制御を説明する。セキュリティモジュールＳＭ１の送出制御部２５は、現時点で復号しているスクランブル鍵Ｋｓの再生手順番号と、次のスクランブル鍵Ｋｓの再生手順番号とを比較し、現時点で復号しているスクランブル鍵Ｋｓの再生手順番号と次のスクランブル鍵Ｋｓの再生手順番号とが同一か、現時点で復号しているスクランブル鍵Ｋｓの再生手順番号に１を加算したものと等しい場合に、復号したスクランブル鍵Ｋｓを送出部２３からコンテンツ利用制御受信装置５に送出させる。

【００８１】いずれの場合にも該当しない際には、送出制御部２５は、コンテンツの再生順序が制限されている旨のエラーメッセージ（エラー信号）を送出部２３からコンテンツ利用制御受信装置５に送出させる。これにより、スクランブル鍵ＫｓがセキュリティモジュールＳＭ１からコンテンツ利用制御受信装置５に送出された場合には、図４中の再生例Aに示したように当該装置５で暗号化コンテンツがコンテンツデスクランブル１５でデスクランブルされ、コンテンツを視聴することができる。

【００８２】また、コンテンツが記憶部１７に記憶させている際に、図４中の再生例Ａ１に示したように、シーンAの一部分シーンＡ１、シーンCの一部分シーンＣ１、シーンEの一部分シーンＥ１を順次ノンリニアに再生しようとする場合を説明する。この場合、シーンＡ１では、再生手順番号が１であるので、送出制御部２５は、スクランブル鍵Ｋｓ（Ｋｓ１１からＫｓ１ｎのいずれか）を送出部２３からコンテンツ利用制御受信装置５に送出させ、コンテンツ利用制御受信装置５では、受信したスクランブル鍵Ｋｓによりコンテンツ（シーンＡ１）をデスクランブルする。

【００８３】ところが、次のシーンＣ１では、再生手順番号が６であるので、送出制御部２５は、スクランブル鍵Ｋｓ（Ｋｓ３１からＫｓ３ｎのいずれか）を送出部２３からコンテンツ利用制御受信装置５に送出させない。このため、コンテンツ利用制御受信装置５では、コンテンツ（シーンＣ１）をデスクランブルすることができない。それゆえ、再生手順番号２、３、４、５が付されているシーンBをデスクランブルしてからシーンＣ１をデスクランブルする必要が生じる。同様に、再生手順番号７、８、９が付されているシーンDをデスクランブルしてからでないとシーンＥ１をデスクランブルすることができない。

【００８４】つまり、コンテンツ利用制御受信装置５において、シーンAからシーンCにノンリニアに再生しようとする場合には、シーンCを再生する際の再生手順番号が不明であるので、再生手順番号を得るために、必ず、シーンBを再生する必要がある。これにより、シーンBであるＣＭをスキップさせてコンテンツを視聴することを防止することができる。すなわち、コンテンツ利用制御受信装置５のユーザのコンテンツの視聴を送信側で制御することができる。

【００８５】（コンテンツの視聴制御（利用制御；再生手順番号の利用の仕方）の例２）また、スクランブル鍵関連情報に含まれる再生手順番号の利用の仕方について補足説明する。例えば、コンテンツ（シーンA～E）がドラマである場合、シーンAからシーンDまでは、各シーンA～Dに同じ再生手順番号１を付しておき、シーンE（ドラマのクライマックス）のみ、再生手順番号を数秒間隔で増加させるように再生手順番号２、３、４、５、６と付しておけば、シーンAからシーンDまでは、コンテンツ利用制御受信装置５（当該装置５に接続される表示装置（図示せず））で自由に視聴できるが、コンテンツ利用制御受信装置５のユーザがシーンEのみ最初に再生させて視聴することを防止することができる。

【００８６】或いは、ドラマ（コンテンツ）に出演している出演者のインタビューの映像をシーンEに含ませて

おき、シーンAからシーンDまですべて視聴したユーザのみシーンEを視聴できるといった視聴制御も可能である。つまり、シーンE（コンテンツの最後）に視聴者が最も視聴したいシーンを含ませておくことで、それ以前のシーンAからシーンD（CM等を含む）を視聴者に積極的に視聴させることができる。

【0087】（コンテンツの視聴制御（利用制御）の例3）一方、コンテンツ鍵関連情報に含まれている視聴制御フラグがオフの場合には、図5中の再生例B1に示したように、再生手順番号に関係なく、コンテンツを再生することができる。つまり、再生例Bに示したようなシーンAからシーンEまでの連続再生ではなく、シーンAの一部であるシーンA1と、シーンCの一部であるシーンC1と、シーンEの一部であるシーンE1とを順次連続再生することができる。

【0088】これによれば、例えば、無料コンテンツを放送する無料放送時には、コンテンツ鍵関連情報に含まれている視聴制御フラグをオンにしたコンテンツ鍵Kcにより、コンテンツ利用制御受信装置5のユーザにコンテンツを視聴させる。すると、当該ユーザは、コンテンツに含まれているCM等をスキップさせることができない。この際に、当該ユーザがコンテンツに含まれているCM等のスキップを望む場合、通信回線等を用いて、一定の料金を送信側のコンテンツ利用制御送信装置3を所有する放送事業者に支払う契約をすると、当該装置3から視聴制御フラグをオフにしたコンテンツ鍵Kc（コンテンツ鍵関連情報）が当該通信回線を介して送信されるようにすることも可能である。この視聴制御フラグをオフにしたコンテンツ鍵Kcを入手したユーザは視聴制限なく（当該コンテンツに限り）コンテンツを利用することができる。このため、無料放送時においても、送信側の放送事業者の意図するコンテンツの視聴（CM等をスキップさせない等の利用制御）を受信側のユーザに行わせることができる。

【0089】（コンテンツの視聴制御（利用制御；複数のワーク鍵）の例4）さらにまた、コンテンツを送信する送信側の放送事業者は、予め、複数の種類のワーク鍵Kw（Kw1、Kw2・・・）を準備しておく（コンテンツ利用制御送信装置3の記憶部11のワーク鍵データベースに記憶）。そして、放送事業者は無料でコンテンツを受信しているコンテンツ利用制御受信装置5のユーザには、ワーク鍵Kw1を、放送事業者に定額料金を支払ってコンテンツを受信しているコンテンツ利用制御受信装置5のユーザには、ワーク鍵Kw2を、セキュリティモジュールSM1に記憶させて、それぞれのユーザに配布しておく。

【0090】その後、コンテンツ利用制御送信装置3からコンテンツ送出時（多重化暗号コンテンツ）に、ワーク鍵Kw1で暗号化されているコンテンツ鍵関連情報（視聴制御フラグはオン）およびワーク鍵Kw2で暗号化されているコンテンツ鍵関連情報（視聴制御フラグはオフ）を併せて送出すれば、ユーザとの契約状況に応じた視聴制御を行うことができる。

【0091】また、図4、図5に示したコンテンツの視聴制御（利用制御）の例では、再生手順番号を1ずつ増加させたが、シーンAからシーンDまでは、図4、図5に示したように再生手順番号を付しておき、シーンEのみ再生手順番号20を付しておくと、送信側で送出されるコンテンツ鍵Kcを含むコンテンツ鍵関連情報（視聴制御フラグはオン）では、シーンEを視聴することができない。この際に、当該ユーザがシーンEの視聴を望む場合、通信回線等を用いて、一定の料金を送信側のコンテンツ利用制御送信装置3を所有する放送事業者に支払う契約をすると、当該装置3から視聴制御フラグをオフにしたコンテンツ鍵Kc（コンテンツ鍵関連情報）が当該通信回線を介して送信されるようにすることも可能である。

【0092】（コンテンツ利用制御受信装置の動作1（記憶後のコンテンツ、ノンリニア再生））図6を参照して、コンテンツ利用制御受信装置5の記憶部17に記憶されているコンテンツを視聴制御する際の動作を説明する。なお、このシーケンスチャートでは、コンテンツがファイルとして記憶部17に記憶されており、当該コンテンツが冒頭から再生されることを想定している。

【0093】コンテンツ利用制御受信装置5の分離部13で多重化暗号コンテンツが分離され暗号化コンテンツ鍵関連情報（コンテンツ鍵Kcを含む）が得られ（S1）、この暗号化コンテンツ鍵関連情報がセキュリティモジュールSM1に送出される。この暗号化コンテンツ鍵関連情報を受信したセキュリティモジュールSM1では、当該暗号化コンテンツ鍵関連情報に含まれているコンテンツ鍵Kcおよび視聴制御フラグが復号される（S2）。

【0094】そして、復号された視聴制御フラグがオンであるかオフであるかが判断され（S3）、復号された視聴制御フラグがオフであると判断された場合には、多重化暗号コンテンツが分離されて得られた暗号化関連情報がコンテンツ利用制御受信装置5からセキュリティモジュールSM1に送出される（S4）。この暗号化関連情報を受信したセキュリティモジュールSM1では、当該暗号化関連情報に含まれている暗号化スクランブル鍵Ksが復号され（S5）、復号されたスクランブル鍵Ksがコンテンツ利用制御受信装置5に送出される（S6）。スクランブル鍵Ksを受信したコンテンツ利用制御受信装置5では、コンテンツデスクランブル部15で、コンテンツ（暗号化コンテンツ）が復号される（S7）。

【0095】S3にて、復号された視聴制御フラグがオンであると判断された場合には、多重化暗号コンテンツが分離されて得られた暗号化関連情報（スクランブル鍵

Ｋｓと再生手順番号を含む）がコンテンツ利用制御受信装置５からセキュリティモジュールＳＭ１に送出される（Ｓ８）。この暗号化関連情報を受信したセキュリティモジュールＳＭ１では、当該暗号化関連情報に含まれている暗号化スクランブル鍵Ｋｓおよび再生手順番号が復号される（Ｓ９）。

【００９６】そして、復号された再生手順番号の数値と記憶部Ｎに記憶されている数値（初期値は１）とが比較され、再生手順番号の数値が記憶部Ｎに記憶されている数値ｎ以下かどうかが判断される（Ｓ１０）。比較判断された結果、再生手順番号の数値が記憶部Ｎに記憶されている数値ｎ以下であると判断された場合には、コンテンツ利用制御受信装置５にスクランブル鍵Ｋｓが送出され（Ｓ１１）、このスクランブル鍵Ｋｓを受信したコンテンツ利用制御受信装置５では、コンテンツデスクランブル部１５で、暗号化コンテンツが復号される（Ｓ１２）。

【００９７】Ｓ１０にて、再生手順番号の数値が記憶部Ｎに記憶されている数値ｎ以下であると判断されない場合には、再生手順番号の数値が数値ｎに１加算した値であるかどうかが判断される（Ｓ１３）。再生手順番号の数値が数値ｎに１加算した値であると判断されない場合には、スクランブル鍵Ｋｓの送出が中断され、コンテンツ利用制御受信装置５においてエラー処理が行われる（Ｓ１４）。このエラー処理はセキュリティモジュールＳＭ１がコンテンツ利用制御受信装置５に対して暗号化コンテンツを復号できない旨のエラー番号（エラー情報）を送出することによって実行される。

【００９８】Ｓ１３にて、再生手順番号の数値が数値ｎに１加算した値であると判断された場合には、この数値ｎが記憶部Ｎに記憶され（Ｓ１５）、コンテンツ利用制御受信装置５にスクランブル鍵Ｋｓが送出され（Ｓ１１）、このスクランブル鍵Ｋｓを受信したコンテンツ利用制御受信装置５では、コンテンツデスクランブル部１５で、暗号化コンテンツが復号される（Ｓ１２）。

【００９９】これらの動作によれば、コンテンツは、暗号化関連情報（スクランブル鍵関連情報）に含まれている再生手順番号（再生順序制御情報；利用制御情報の一つ）に従った場合のみ復号されるので、当該コンテンツに一体的に含まれているＣＭのスキップ等を防止することができると共に、巻き戻し等により一度視聴した区間（コンテンツの一部）は、自由にノンリニア再生することができる。

【０１００】（コンテンツ利用制御受信装置の動作２（記憶後のコンテンツ、再生手順番号順））図７を参照して、コンテンツ利用制御受信装置５の記憶部１７に記憶されているコンテンツを視聴制御する際の動作を説明する。なお、このシーケンスチャートでは、コンテンツがファイルとして記憶部１７に記憶されており、当該コンテンツが冒頭から再生されることを想定している。

【０１０１】コンテンツ利用制御受信装置５の分離部１３で多重化暗号コンテンツが分離され暗号化コンテンツ鍵関連情報（コンテンツ鍵Ｋｃを含む）が得られ（Ｓ２１）、この暗号化コンテンツ鍵関連情報がセキュリティモジュールＳＭ１に送出される。この暗号化コンテンツ鍵関連情報を受信したセキュリティモジュールＳＭ１では、当該暗号化コンテンツ鍵関連情報に含まれているコンテンツ鍵Ｋｃおよび視聴制御フラグが復号される（Ｓ２２）。

【０１０２】そして、復号された視聴制御フラグがオンであるかオフであるかが判断され（Ｓ２３）、復号された視聴制御フラグがオフであると判断された場合には、多重化暗号コンテンツが分離されて得られた暗号化関連情報がコンテンツ利用制御受信装置５からセキュリティモジュールＳＭ１に送出される（Ｓ２４）。この暗号化関連情報を受信したセキュリティモジュールＳＭ１では、当該暗号化関連情報に含まれている暗号化スクランブル鍵Ｋｓが復号され（Ｓ２５）、復号されたスクランブル鍵Ｋｓがコンテンツ利用制御受信装置５に送出される（Ｓ２６）。スクランブル鍵Ｋｓを受信したコンテンツ利用制御受信装置５では、コンテンツデスクランブル部１５で、暗号化コンテンツが復号される（Ｓ２７）。

【０１０３】Ｓ２３にて、復号された視聴制御フラグがオンであると判断された場合には、多重化暗号コンテンツが分離されて得られた暗号化関連情報がコンテンツ利用制御受信装置５からセキュリティモジュールＳＭ１に送出される（Ｓ２８）。この暗号化関連情報を受信したセキュリティモジュールＳＭ１では、当該暗号化関連情報に含まれている暗号化スクランブル鍵Ｋｓおよび再生手順番号が復号される（Ｓ２９）。

【０１０４】そして、復号された再生手順番号の数値と記憶部Ｎに記憶されている数値（初期値は１）とが比較され、同じ数値であるかどうかが判断される（Ｓ３０）。比較判断された結果、再生手順番号の数値が記憶部Ｎに記憶されている数値ｎと同じであると判断された場合には、コンテンツ利用制御受信装置５にスクランブル鍵Ｋｓが送出され（Ｓ３１）、このスクランブル鍵Ｋｓを受信したコンテンツ利用制御受信装置５では、コンテンツデスクランブル部１５で、暗号化コンテンツが復号される（Ｓ３２）。

【０１０５】Ｓ３０にて、再生手順番号の数値が記憶部Ｎに記憶されている数値ｎと同じであると判断されない場合には、再生手順番号の数値が数値ｎ未満か、または再生手順番号の数値が数値ｎに１加算した値であるかどうかが判断される（Ｓ３３）。再生手順番号の数値が数値ｎ未満か、再生手順番号の数値が数値ｎに１加算した値であると判断されない場合には、スクランブル鍵Ｋｓの送出が中断され、コンテンツ利用制御受信装置５においてエラー処理が行われる（Ｓ３４）。このエラー処理はセキュリティモジュールＳＭ１がコンテンツ利用制御

受信装置５に対して暗号化コンテンツを復号できない旨のエラー番号（エラー情報）を送出することによって実行される。

【０１０６】Ｓ３３にて、再生手順番号の数値が数値ｎ未満か、再生手順番号の数値がｎに１加算した値であると判断された場合には、この数値ｎが記憶部Ｎに記憶され（Ｓ３５）、コンテンツ利用制御受信装置５にスクランブル鍵Ｋｓが送出され（Ｓ３１）、このスクランブル鍵Ｋｓを受信したコンテンツ利用制御受信装置５では、コンテンツデスクランブル部１５で、暗号化コンテンツが復号される（Ｓ３２）。

【０１０７】これらの動作によれば、コンテンツは、暗号化関連情報（スクランブル鍵関連情報）に含まれている再生手順番号（再生順序制御情報；利用制御情報の一つ）に従った場合のみ復号されるので、当該コンテンツに一体的に含まれているＣＭのスキップ等を防止することができる。また、この動作では、再生手順番号の数値が記憶部Ｎに記憶されている数値ｎよりも小さい場合であっても、記憶部Ｎに再生手順番号を記憶させる手順（Ｓ３３、Ｓ３４）を追加している。このため、巻き戻し等により一度視聴した区間（コンテンツの一部）であっても、同様に再生手順番号に従った視聴制限することができる。

【０１０８】（コンテンツ利用制御受信装置の動作３（リアルタイムのコンテンツ））図８を参照して、コンテンツ利用制御受信装置５でリアルタイムに受信しているコンテンツを視聴制御する際の動作を説明する。この動作はリアルタイムに受信しているコンテンツと記憶部１７に記憶されたコンテンツの両方を考慮した動作で、放送されているコンテンツを途中から記憶して視聴する場合や、記憶しつつ視聴する際に一部分のコンテンツが記憶できなかったり視聴できなかった場合に対応するための動作である。

【０１０９】コンテンツ利用制御受信装置５の分離部１３で多重化暗号コンテンツが分離され暗号化コンテンツ鍵関連情報（コンテンツ鍵Ｋｃを含む）が得られ（Ｓ４１）、この暗号化コンテンツ鍵関連情報がセキュリティモジュールＳＭ１に送出される。この暗号化コンテンツ鍵関連情報を受信したセキュリティモジュールＳＭ１では、当該暗号化コンテンツ鍵関連情報に含まれているコンテンツ鍵Ｋｃおよび視聴制御フラグが復号される（Ｓ４２）。

【０１１０】そして、復号された視聴制御フラグがオンであるかオフであるかが判断され（Ｓ４３）、復号された視聴制御フラグがオフであると判断された場合には、多重化暗号コンテンツが分離されて得られた暗号化関連情報がコンテンツ利用制御受信装置５からセキュリティモジュールＳＭ１に送出される（Ｓ４４）。この暗号化関連情報を受信したセキュリティモジュールＳＭ１では、当該暗号化関連情報に含まれている暗号化スクランブル鍵Ｋｓが復号され（Ｓ４５）、復号されたスクランブル鍵Ｋｓがコンテンツ利用制御受信装置５に送出される（Ｓ４６）。スクランブル鍵Ｋｓを受信したコンテンツ利用制御受信装置５では、コンテンツデスクランブル部１５で、暗号化コンテンツが復号される（Ｓ４７）。

【０１１１】Ｓ４３にて、復号された視聴制御フラグがオンであると判断された場合には、多重化暗号コンテンツが分離されて得られた暗号化関連情報がコンテンツ利用制御受信装置５からセキュリティモジュールＳＭ１に送出される（Ｓ４８）。この暗号化関連情報を受信したセキュリティモジュールＳＭ１では、当該暗号化関連情報に含まれている暗号化スクランブル鍵Ｋｓおよび再生手順番号が復号される（Ｓ４９）。

【０１１２】そして、最初に受信した再生手順番号の数値を記憶部Ｎに記憶させておき（Ｓ５０）、復号された再生手順番号の数値と記憶部Ｎに記憶されている数値（最初に受信した際の数値）とが比較され、同じ数値であるかどうかが判断される（Ｓ５１）。比較判断された結果、再生手順番号の数値が記憶部Ｎに記憶されている数値ｎと同じであると判断された場合には、コンテンツ利用制御受信装置５にスクランブル鍵Ｋｓが送出され（Ｓ５２）、このスクランブル鍵Ｋｓを受信したコンテンツ利用制御受信装置５では、コンテンツデスクランブル部１５で、暗号化コンテンツが復号される（Ｓ５３）。

【０１１３】Ｓ５１にて、再生手順番号の数値が記憶部Ｎに記憶されている数値ｎと同じであると判断されない場合には、再生手順番号の数値が数値ｎ未満か、または再生手順番号の数値が数値ｎに１加算した値であるかどうかが判断される（Ｓ５４）。再生手順番号の数値が数値ｎ未満か、再生手順番号の数値が数値ｎに１加算した値であると判断されない場合には、スクランブル鍵Ｋｓの送出が中断され、コンテンツ利用制御受信装置５においてエラー処理が行われる（Ｓ５５）。このエラー処理はセキュリティモジュールＳＭ１がコンテンツ利用制御受信装置５に対して暗号化コンテンツを復号できない旨のエラー番号（エラー情報）を送出することによって実行される。

【０１１４】Ｓ５４にて、再生手順番号の数値が数値ｎ未満か、再生手順番号の数値がｎに１加算した値であると判断された場合には、この数値ｎが記憶部Ｎに記憶され（Ｓ５６）、コンテンツ利用制御受信装置５にスクランブル鍵Ｋｓが送出され（Ｓ５２）、このスクランブル鍵Ｋｓを受信したコンテンツ利用制御受信装置５では、コンテンツデスクランブル部１５で、暗号化コンテンツが復号される（Ｓ５３）。

【０１１５】これらの動作によれば、デスクランブルしたいコンテンツの、最初に受信された再生手順番号の数値を記憶部Ｎの初期値として設定しているので、リアルタイムに受信しているコンテンツ（デスクランブルした

いコンテンツ）を途中から視聴したり、コンテンツの冒頭から記憶部１７に記憶していないコンテンツの再生が可能になり、再生手順番号に従ったコンテンツの視聴制限（視聴制御）を行うことができる。

【０１１６】（視聴制御フラグに関して補足）ここまでの説明において、視聴制御フラグをオン・オフのみの１ビットの利用制御情報としてきた。しかし、視聴制御フラグのビット数を増加させて、例えば、視聴制御フラグが０の時は、視聴制御自体をオフ、視聴制御フラグが１の時は図７に示したシーケンスチャートに基づく制御、視聴制御フラグが２の時は、図８に示したシーケンスチャートに基づく制御とすることも可能である。

【０１１７】この実施の形態では以下の効果を奏す。コンテンツ利用制御送信装置３では、スクランブル鍵Ｋｓを用いて、コンテンツスクランブル部７（７ａ）でコンテンツが暗号化され暗号化コンテンツとされる。一方、暗号化器７ｂで、記憶部１１に記憶されているコンテンツ鍵Ｋｃによって、少なくとも再生手順番号およびスクランブル鍵Ｋｓを含む関連情報が暗号化し暗号化関連情報とされる。また、暗号化器７ｃで、記憶部１１に記憶されているワーク鍵Ｋｗによって、少なくとも視聴制御フラグおよびコンテンツ鍵Ｋｃを含む当該コンテンツ鍵Ｋｃに関するコンテンツ鍵関連情報が暗号化され暗号化コンテンツ鍵関連情報とされる。さらに、暗号化器７ｄで、マスター鍵によって、少なくともワーク鍵Ｋｗを含むワーク鍵Ｋｗに関するワーク鍵関連情報が暗号化され暗号化ワーク鍵関連情報とされる。そして、多重化部９で、これらが多重化暗号コンテンツとされ、送信される。

【０１１８】コンテンツ利用制御受信装置５では、分離部１３で、暗号化コンテンツ、暗号化関連情報、暗号化コンテンツ鍵関連情報、暗号化ワーク鍵関連情報が送信側のコンテンツ利用制御送信装置３で多重化された多重化暗号コンテンツが受信され、これらが分離される。そしてまた、ここで分離された暗号化ワーク鍵関連情報がマスター鍵Ｋｍにより復号器１５ａで復号されワーク鍵Ｋｗが得られ、復号器１５ｂで、得られたワーク鍵Ｋｗで暗号化コンテンツ鍵Ｋｃおよび暗号化されている視聴制御フラグが復号され、コンテンツ鍵Ｋｃおよび視聴制御フラグが得られる。この視聴制御情フラグに基づいて、復号器１５ｃで、暗号化スクランブル鍵Ｋｓおよび暗号化されている再生手順番号が復号され、この再生手順番号に基づいて、コンテンツデスクランブル部１５（１５ｄ）にて、スクランブル鍵Ｋｓで暗号化コンテンツが復号され、コンテンツが得られる。

【０１１９】つまり、コンテンツ利用制御送信装置３およびコンテンツ利用制御受信装置５においてコンテンツの暗号化、復号に、暗号化関連情報（スクランブル鍵関連情報）に含まれている再生手順番号によりグループ化されたスクランブル鍵Ｋｓを用いることで、受信側の受信機が不正に改造されたり不正に製造されたものであっても、コンテンツの不正利用を防止することができ、さらに送信側の放送局（放送事業者）が、受信側でのコンテンツの視聴順序を指定する、コンテンツの利用制御を実現することができる。

【０１２０】また、送信側の放送局が設定した再生手順番号（再生順序制御情報）により、あるシーンやＣＭのスキップを受信側に委ねず、送信側で制御することができ、コンテンツの制作者（放送局（放送事業者））の意図した通りに、受信側でコンテンツを利用させることができる。さらに、ＣＭ等の広告収入を主な収入源にしている民間の無料放送事業者は、広告収入を確保しながら、コンテンツのノンリニア再生や、メタデータによるコンテンツ検索等の便利な新サービスを視聴者に提供することができる。

【０１２１】以上、一実施形態に基づいて本発明を説明したが、本発明はこれに限定されるものではない。コンテンツ利用制御送信装置３、コンテンツ利用制御受信装置５の各構成の処理を、一般的なプログラム言語で記述したコンテンツ送信プログラム、コンテンツ受信プログラムとみなすことも可能である。この場合も、コンテンツ利用制御送信装置３、コンテンツ利用制御受信装置５で得られる効果と同様の効果が得られる。さらに、このプログラムを記憶媒体（フレキシブルディスク、ＣＤ－ＲＯＭ等）に記憶し、流通させることも可能である。

【０１２２】

【発明の効果】請求項１記載の発明によれば、スクランブル鍵によって暗号化された暗号化コンテンツと、共通鍵によって暗号化された暗号化関連情報とが、多重化ステップにおいて多重化され多重化暗号コンテンツとされ送信される。このため、受信側の受信装置が不正に改造されたり不正に製造されたものであっても、スクランブル鍵関連情報内に視聴制御情報が入っているため、仮に視聴制御情報を無視にするために、スクランブル鍵関連情報を無視すると、復号されたスクランブル鍵を得ることができず、また、仮に視聴制御情報のみを取り除こうとしても、視聴制御情報は暗号化されており、取り除くことができないため、コンテンツの不正利用を防止することができる。

【０１２３】請求項２記載の発明によれば、利用制御情報が再生順序制御情報と視聴制御情報との少なくとも一方の情報を含んでいるので、受信側でコンテンツを利用するときに、この情報に従って、送信側の意図するようにコンテンツの利用制御を受信側で行わせることができる。

【０１２４】請求項３記載の発明によれば、スクランブル鍵によって暗号化された暗号化コンテンツと、コンテンツ鍵によって暗号化された暗号化関連情報と、ワーク鍵によって暗号化された暗号化コンテンツ鍵関連情報と、マスター鍵によって暗号化された暗号化ワーク鍵関

連情報が、多重化ステップにおいて多重化され多重化暗号コンテンツとされ送信される。このため、受信側の受信装置が不正に改造されたり不正に製造されたものであっても、スクランブル鍵関連情報内に視聴制御情報が入っているため、仮に視聴制御情報を無視にするために、スクランブル鍵関連情報を無視すると、復号されたスクランブル鍵を得ることができず、また、仮に視聴制御情報のみを取り除こうとしても、視聴制御情報は暗号化されており、取り除くことができないため、コンテンツの不正利用を防止することができる。

【０１２５】請求項４記載の発明によれば、受信された多重化暗号コンテンツが暗号化コンテンツと暗号化関連情報とに分離され、暗号化利用制御情報復号ステップで、暗号化スクランブル鍵および暗号化利用制御情報が復号され、暗号化コンテンツ復号ステップで、復号された利用制御情報に基づいて暗号化コンテンツが復号される。このため、受信側の受信装置が不正に改造されたり不正に製造されたものであっても、スクランブル鍵関連情報内に視聴制御情報が入っているため、仮に視聴制御情報を無視にするために、スクランブル鍵関連情報を無視すると、復号されたスクランブル鍵を得ることができず、また、仮に視聴制御情報のみを取り除こうとしても、視聴制御情報は暗号化されており、取り除くことができないため、コンテンツの不正利用を防止することができる。

【０１２６】請求項５記載の発明によれば、受信された多重化暗号コンテンツが暗号化コンテンツと暗号化関連情報と暗号化コンテンツ鍵関連情報と暗号化ワーク鍵関連情報とに分離され、暗号化ワーク鍵関連情報がマスター鍵で復号され、復号されたワーク鍵で暗号化コンテンツ鍵および暗号化視聴制御情報が復号され、復号された視聴制御情報に基づいて、暗号化スクランブル鍵および暗号化再生順序制御情報が復号され、復号された再生順序制御情報に基づいて、スクランブル鍵で暗号化コンテンツが復号される。このため、受信側の受信装置が不正に改造されたり不正に製造されたものであっても、スクランブル鍵関連情報内に視聴制御情報が入っているため、仮に視聴制御情報を無視にするために、スクランブル鍵関連情報を無視すると、復号されたスクランブル鍵を得ることができず、また、仮に視聴制御情報のみを取り除こうとしても、視聴制御情報は暗号化されており、取り除くことができないため、コンテンツの不正利用を防止することができる。

【０１２７】請求項６記載の発明によれば、スクランブル鍵によって暗号化された暗号化コンテンツと、共通鍵によって暗号化された暗号化関連情報とが、多重化手段において多重化され多重化暗号コンテンツとされ送信される。このため、受信側の受信装置が不正に改造されたり不正に製造されたものであっても、スクランブル鍵関連情報内に視聴制御情報が入っているため、仮に視聴制御情報を無視にするために、スクランブル鍵関連情報を無視すると、復号されたスクランブル鍵を得ることができず、また、仮に視聴制御情報のみを取り除こうとしても、視聴制御情報は暗号化されており、取り除くことができないため、コンテンツの不正利用を防止することができる。

【０１２８】請求項７記載の発明によれば、利用制御情報が再生順序制御情報と視聴制御情報との少なくとも一方の情報を含んでいるので、受信側でコンテンツを利用するときに、この情報に従って、送信側の意図するようにコンテンツの利用制御を受信側で行わせることができる。

【０１２９】請求項８記載の発明によれば、スクランブル鍵によって暗号化された暗号化コンテンツと、コンテンツ鍵によって暗号化された暗号化関連情報と、ワーク鍵によって暗号化された暗号化コンテンツ鍵関連情報と、マスター鍵によって暗号化された暗号化ワーク鍵関連情報が、多重化手段において多重化され多重化暗号コンテンツとされ送信される。このため、受信側の受信装置が不正に改造されたり不正に製造されたものであっても、スクランブル鍵関連情報内に視聴制御情報が入っているため、仮に視聴制御情報を無視にするために、スクランブル鍵関連情報を無視すると、復号されたスクランブル鍵を得ることができず、また、仮に視聴制御情報のみを取り除こうとしても、視聴制御情報は暗号化されており、取り除くことができないため、コンテンツの不正利用を防止することができる。

【０１３０】請求項９記載の発明によれば、受信された多重化暗号コンテンツが暗号化コンテンツと暗号化関連情報とに分離され、暗号化利用制御情報復号手段で、暗号化スクランブル鍵および暗号化利用制御情報が復号され、暗号化コンテンツ復号手段で、復号された利用制御情報に基づいて暗号化コンテンツが復号される。このため、受信側の受信装置が不正に改造されたり不正に製造されたものであっても、スクランブル鍵関連情報内に視聴制御情報が入っているため、仮に視聴制御情報を無視にするために、スクランブル鍵関連情報を無視すると、復号されたスクランブル鍵を得ることができず、また、仮に視聴制御情報のみを取り除こうとしても、視聴制御情報は暗号化されており、取り除くことができないため、コンテンツの不正利用を防止することができる。

【０１３１】請求項１０記載の発明によれば、受信された多重化暗号コンテンツが暗号化コンテンツと暗号化関連情報と暗号化コンテンツ鍵関連情報と暗号化ワーク鍵関連情報とに分離され、暗号化ワーク鍵関連情報がマスター鍵で復号され、復号されたワーク鍵で暗号化コンテンツ鍵および暗号化視聴制御情報が復号され、復号された視聴制御情報に基づいて、暗号化スクランブル鍵および暗号化再生順序制御情報が復号され、復号された再生順序制御情報に基づいて、スクランブル鍵で暗号化コン

テンツが復号される。このため、受信側の受信装置が不正に改造されたり不正に製造されたものであっても、スクランブル鍵関連情報内に視聴制御情報が入っているため、仮に視聴制御情報を無視にするために、スクランブル鍵関連情報を無視すると、復号されたスクランブル鍵を得ることができず、また、仮に視聴制御情報のみを取り除こうとしても、視聴制御情報は暗号化されており、取り除くことができないため、コンテンツの不正利用を防止することができる。

【0132】請求項11記載の発明によれば、コンテンツ利用制御送信プログラムにおいて、スクランブル鍵によって暗号化された暗号化コンテンツと、共通鍵によって暗号化された暗号化関連情報とが、多重化手段において多重化され多重化暗号コンテンツとされ送信される。このため、受信側の受信装置が不正に改造されたり不正に製造されたものであっても、スクランブル鍵関連情報内に視聴制御情報が入っているため、仮に視聴制御情報を無視にするために、スクランブル鍵関連情報を無視すると、復号されたスクランブル鍵を得ることができず、また、仮に視聴制御情報のみを取り除こうとしても、視聴制御情報は暗号化されており、取り除くことができないため、コンテンツの不正利用を防止することができる。

【0133】請求項12記載の発明によれば、コンテンツ利用制御送信プログラムにおいて、利用制御情報が再生順序制御情報と視聴制御情報との少なくとも一方の情報を含んでいるので、受信側でコンテンツを利用するときに、この情報に従って、送信側の意図するようにコンテンツの利用制御を受信側で行わせることができる。

【0134】請求項13記載の発明によれば、コンテンツ利用制御送信プログラムにおいて、スクランブル鍵によって暗号化された暗号化コンテンツと、コンテンツ鍵によって暗号化された暗号化関連情報と、ワーク鍵によって暗号化された暗号化コンテンツ鍵関連情報と、マスター鍵によって暗号化された暗号化ワーク鍵関連情報が、多重化手段において多重化され多重化暗号コンテンツとされ送信される。このため、受信側の受信装置が不正に改造されたり不正に製造されたものであっても、スクランブル鍵関連情報内に視聴制御情報が入っているため、仮に視聴制御情報を無視にするために、スクランブル鍵関連情報を無視すると、復号されたスクランブル鍵を得ることができず、また、仮に視聴制御情報のみを取り除こうとしても、視聴制御情報は暗号化されており、取り除くことができないため、コンテンツの不正利用を防止することができる。

【0135】請求項14記載の発明によれば、コンテンツ利用制御受信プログラムにおいて、受信された多重化暗号コンテンツが暗号化コンテンツと暗号化関連情報とに分離され、暗号化利用制御情報復号手段で、暗号化スクランブル鍵および暗号化利用制御情報が復号され、暗号化コンテンツ復号手段で、復号された利用制御情報に基づいて暗号化コンテンツが復号される。このため、受信側の受信装置が不正に改造されたり不正に製造されたものであっても、スクランブル鍵関連情報内に視聴制御情報が入っているため、仮に視聴制御情報を無視にするために、スクランブル鍵関連情報を無視すると、復号されたスクランブル鍵を得ることができず、また、仮に視聴制御情報のみを取り除こうとしても、視聴制御情報は暗号化されており、取り除くことができないため、コンテンツの不正利用を防止することができる。

【0136】請求項15記載の発明によれば、コンテンツ利用制御受信プログラムにおいて、受信された多重化暗号コンテンツが暗号化コンテンツと暗号化関連情報と暗号化コンテンツ鍵関連情報と暗号化ワーク鍵関連情報とに分離され、暗号化ワーク鍵関連情報がマスター鍵で復号され、復号されたワーク鍵で暗号化コンテンツ鍵および暗号化視聴制御情報が復号され、復号された視聴制御情報に基づいて、暗号化スクランブル鍵および暗号化再生順序制御情報が復号され、復号された再生順序制御情報に基づいて、スクランブル鍵で暗号化コンテンツが復号される。このため、受信側の受信装置が不正に改造されたり不正に製造されたものであっても、スクランブル鍵関連情報内に視聴制御情報が入っているため、仮に視聴制御情報を無視にするために、スクランブル鍵関連情報を無視すると、復号されたスクランブル鍵を得ることができず、また、仮に視聴制御情報のみを取り除こうとしても、視聴制御情報は暗号化されており、取り除くことができないため、コンテンツの不正利用を防止することができる。

【図面の簡単な説明】

【図1】本発明による一実施の形態であるコンテンツ利用制御システム（コンテンツ利用制御送信装置およびコンテンツ利用制御受信装置）のブロック図である。

【図2】コンテンツ利用制御送信装置から送信されるファイルのフォーマット例を説明した説明図である。

【図3】コンテンツ利用制御受信装置およびセキュリティモジュールを説明した説明図である。

【図4】コンテンツに付されている再生手順番号に基づいたコンテンツの視聴制御（視聴制御フラグオン）を説明した説明図である。

【図5】コンテンツに付されている再生手順番号に基づいたコンテンツの視聴制御（視聴制御フラグオフ）を説明した説明図である。

【図6】コンテンツ利用制御受信装置でコンテンツを視聴制御する際の動作（記憶後、ノンリニア再生）を説明したシーケンスチャートである。

【図7】コンテンツ利用制御受信装置でコンテンツを視聴制御する際の動作（記憶後、再生手順番号順）を説明したシーケンスチャートである。

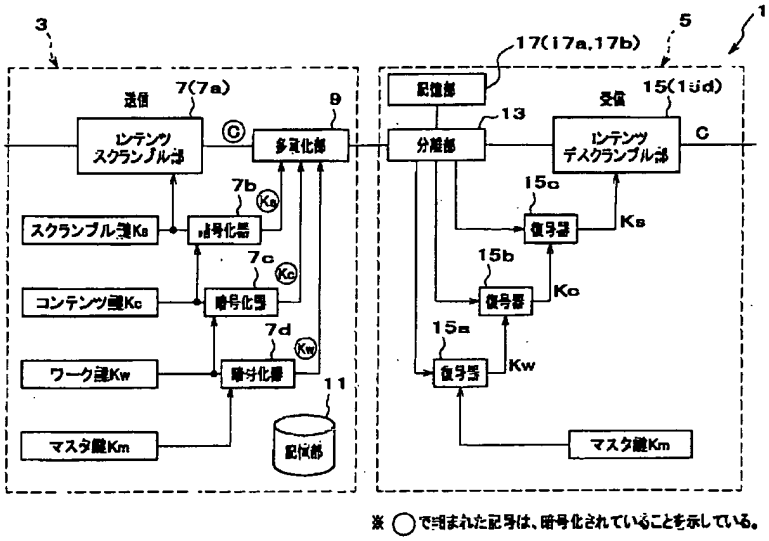
【図8】コンテンツ利用制御受信装置でコンテンツを視

聴制御する際の動作（リアルタイム）を説明したシーケンスチャートである。

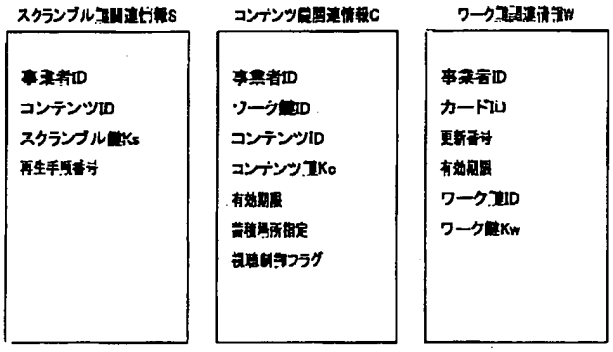
【符号の説明】

1　コンテンツ利用制御システム
3　コンテンツ利用制御送信装置
5　コンテンツ利用制御受信装置
7　コンテンツスクランブル部
9　多重化部
11、17　記憶部
13　分離部
15　コンテンツデスクランブル部

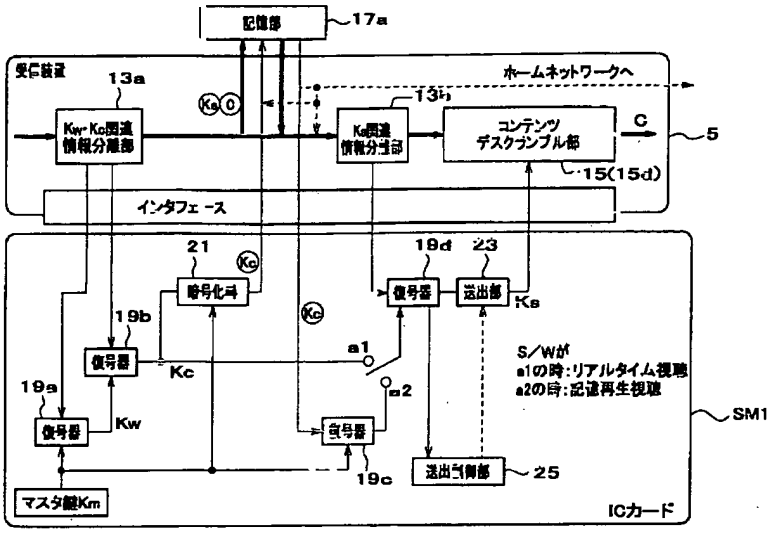
【図1】



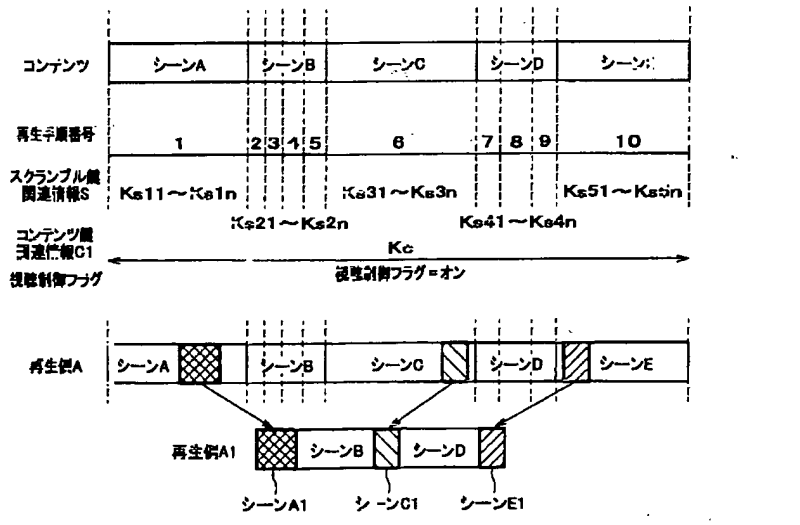
【図2】



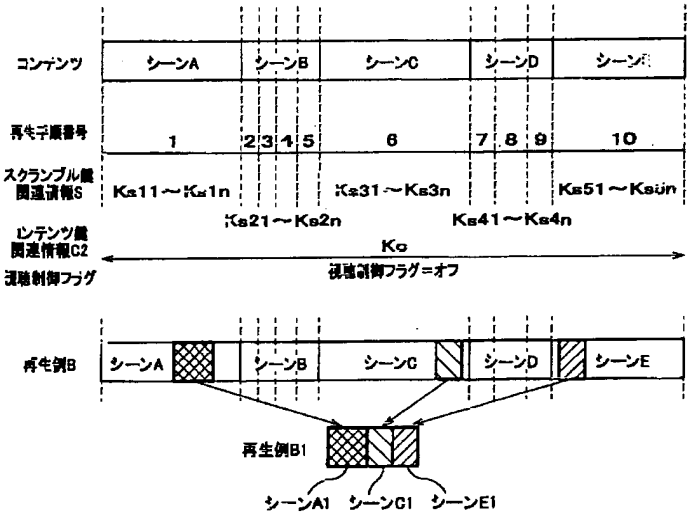
【図3】


記憶部
17a
受信装置
13a
ホームネットワークへ
Kw・Ks関連情報分離部
Ks関連情報分離部
13b
コンテンツデスクランブル部
C
5
15(15d)
インタフェース
21
暗号化器
19d
23
復号器
送出部
Ks
19b
復号器
Kc
a1
a2
S/Wが
a1の時:リアルタイム視聴
a2の時:記憶再生視聴
SM1
19a
復号器
Kw
19c
送出制御部
25
マスタ鍵Km
ICカード

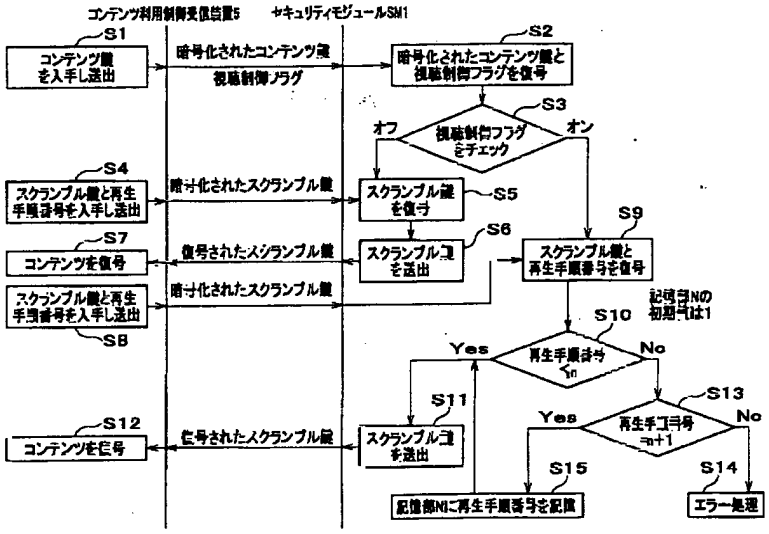
【図4】


コンテンツ
シーンA
シーンB
シーンC
シーンD
再生手順番号
1
2
3
4
5
6
7
8
9
10
スクランブル鍵関連情報S
Ks11～Ks1n
Ks21～Ks2n
Ks31～Ks3n
Ks41～Ks4n
Ks51～Ks5n
コンテンツ鍵関連情報C1
Kc
視聴制御フラグ
視聴制御フラグ=オン
再生例A
シーンE
再生例A1
シーンA1
シーンC1
シーンE1

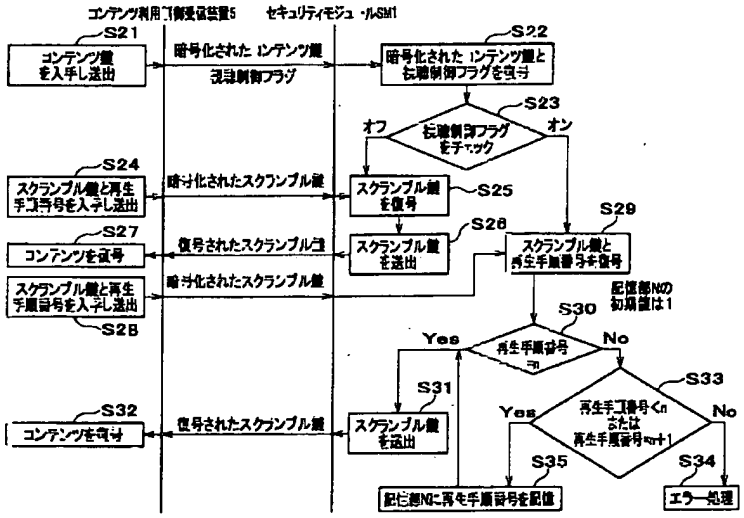
【図5】


コンテンツ
シーンA
シーンB
シーンC
シーンD
シーンE
再生手順番号
1
2
3
4
5
6
7
8
9
10
スクランブル鍵関連情報S
Ks11～Ks1n
Ks21～Ks2n
Ks31～Ks3n
Ks41～Ks4n
Ks51～Ksun
コンテンツ鍵関連情報C2
Kc
視聴制御フラグ
視聴制御フラグ=オフ
再生例B
再生例B1
シーンA1
シーンC1
シーンE1

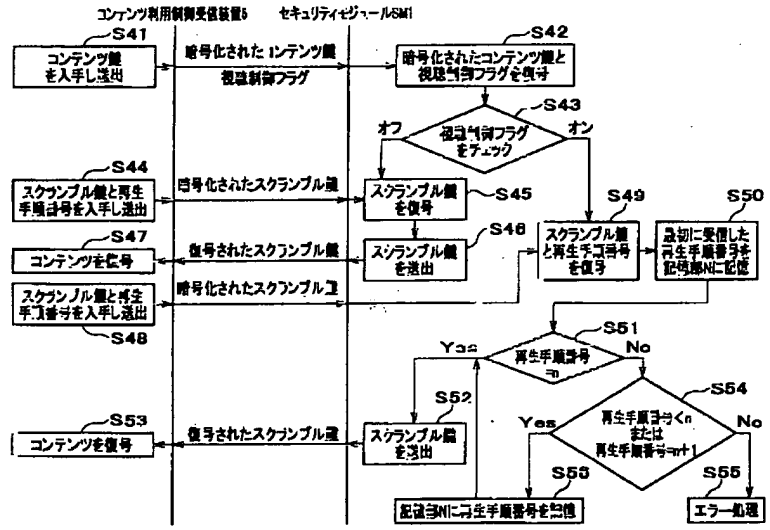
【図6】


コンテンツ利用制御受信装置5
セキュリティモジュールSM1
S1
コンテンツ鍵を入手し送出
暗号化されたコンテンツ鍵
視聴制御フラグ
S2
暗号化されたコンテンツ鍵と視聴制御フラグを復号
S3
視聴制御フラグをチェック
オフ
オン
S4
スクランブル鍵と再生手順番号を入手し送出
暗号化されたスクランブル鍵
S5
スクランブル鍵を復号
S6
スクランブル鍵を送出
S7
コンテンツを復号
復号されたスクランブル鍵
暗号化されたスクランブル鍵
スクランブル鍵と再生手順番号を入手し送出
S8
S9
スクランブル鍵と再生手順番号を復号
記憶部Nの初期値は1
S10
再生手順番号=n
Yes
No
S11
スクランブル鍵を送出
S12
コンテンツを復号
復号されたスクランブル鍵
S13
再生手順番号=n+1
Yes
No
S15
記憶部N1に再生手順番号を記憶
S14
エラー処理

【図7】



【図8】



フロントページの続き

(51)Int.Cl.[7]	識別記号	F I	(参考)
H04N 7/167			

(72)発明者 上原 年博
東京都世田谷区砧一丁目10番11号 日本放送協会 放送技術研究所内

(72)発明者 難波 誠一
東京都世田谷区砧一丁目10番11号 日本放送協会 放送技術研究所内

(72)発明者　奥田　治雄
東京都世田谷区砧一丁目10番11号　日本放送協会　放送技術研究所内

Fターム(参考)　5C063 AB03 AB11 DA13 DA20
5C064 BC22 BC25 CA14 CB01 CC04
5J104 AA16 BA03 EA07 EA18 NA02
NA03 PA05

【発明の名称】

コンテンツ利用制御送信方法、コンテンツ利用制御受信方法およびコンテンツ利用制御送信装置、コンテンツ利用制御受信装置ならびにコンテンツ利用制御送信プログラム、コンテンツ利用制御受信プログラム